Ministero dell'Università e della Ricerca

Segretariato Generale

Direzione Generale per il coordinamento e la valorizzazione della ricerca e dei suoi risultati

PRIN: PROGETTI DI RICERCA DI RILEVANTE INTERESSE NAZIONALE – Bando 2020
Prot. 20202FCJMH

PART A

1. Research project title

Noninterference and Reversibility Analysis in Private Blockchains (NiRvAna)

2. Duration (months)

36 months

3. Main ERC field

PE - Physical Sciences and Engineering

4. Possible other ERC field

5. ERC subfields

1.	PE6_4 Theoretical computer science, formal methods, and quantum computing
2.	
3.	

6. Keywords

nº	Testo inglese
1.	theoretical computer science
2.	formal methods in computer science
3.	parallel and distributed systems
4.	stochastic processes
5.	computer security and privacy
6.	reversible computing

7. Principal Investigator

BERNARDO (Surname)	**MARCO** (Name)
Professore Ordinario (L. 240/10) (Qualification)	
12/02/1970 (Date of birth)	**BRNMRC70B12A944M** (Personal identification code)
Università degli Studi di Urbino Carlo Bo (Organization)	
0722-304416 (Phone number)	**marco.bernardo@uniurb.it** (E-mail address)

8. List of the Research Units

nº	Associated Investigator	Qualification	University/ Research Institution	e-mail address
1.	BERNARDO Marco	Professore Ordinario (L. 240/10)	Università degli Studi di Urbino Carlo Bo	marco.bernardo@uniurb.it
2.	ROSSI Sabina	Professore Associato (L. 240/10)	Università "Ca' Foscari" VENEZIA	srossi@dsi.unive.it
3.	PIAZZA Carla	Professore Associato confermato	Università degli Studi di UDINE	carla.piazza@uniud.it

9 - Substitute Principal Investigator (To be identified among one of the research units participating in the project).

ROSSI (Surname)	**SABINA** (Name)
Professore Associato (L. 240/10) (Qualification)	
07/12/1966 (Date of birth)	**RSSSBN66T47E512S** (Personal identification code)
Università "Ca' Foscari" VENEZIA (Organization)	
041 2348422 (Phone number)	**srossi@dsi.unive.it** (E-mail address)

10. Brief description of the proposal

Distributed computing has by now become a pervasive technology due to the widespread adoption of electronic devices connected by the Internet infrastructure, which are used by individuals, companies, and institutions to perform an increasing number of activities in a digital mode. One of the most prominent examples over the last decade is blockchain technology. This is a distributed ledger that permanently records transactions taking place among untrusted parties in a decentralized and disintermediated environment, which was devised to avoid the double spending problem in virtual currency platforms.

A number of shortcomings affect public, permissionless blockchains, including the excessive energy consumption required by the consensus protocol and conflicts between data immutability and regulations. In the specific case of innovative payment methods, there are also risks of losing monetary sovereignty and undermining financial stability, as witnessed by the fact that many central banks are exploring the issuance of what is called central bank digital currency (CBDC). For these reasons private, permissioned blockchains are getting momentum, as they could ultimately give businesses a greater degree of control.

Developing complex distributed systems like private blockchains is extremely challenging in terms of guaranteeing high levels of proper functioning, data protection, and quality of service. It even becomes a critical issue in CBDC platforms, where errors, data breaches, and poor performance may have economical and social consequences hard to estimate. This calls for a model-based approach in the early design stages so as to enable system property prediction.

The NiRvAna project is about the use of formal methods for the compositional modeling of functional and non-functional aspects of the behavior and the structure of private blockchains. On the analysis side, we will focus on relevant properties such as noninterference and reversibility. The former is concerned with the absence of information leakage, due to qualitative or quantitative covert channels, from the private blockchain governance to permissioned users. The latter deals with undoing transactions, because of regulation compliance, in a way that timely brings the system in a previous consistent state. This will be accomplished by developing or extending modeling languages, analysis techniques, and software tools according to an integrated view of correctness, security, and performance objectives.

11. Total cost of the research project identified by items

Associated Investigator	item A.1	item A.2.1	item B	item C	item D	item E	sub-total	Total
BERNARDO Marco	112.108	50.000	97.265	12.000	0	20.000	291.373	**291.373**

ROSSI Sabina	89.720	50.000	83.832	10.000	0	15.000	248.552	**248.552**
PIAZZA Carla	86.092	50.000	81.655	10.000	0	15.000	242.747	**242.747**
Total	**287.920**	**150.000**	**262.752**	**32.000**	**0**	**50.000**	**782.672**	**782.672**

N.B. The Item B and TOTAL columns will be filled in automatically

- item A.1: enhancement of months/person of permanent employees
- item A.2.1: cost of contracts of non-employees, specifically to recruit
- item B: overhead (flat rate equal to 60% of the total personnel cost, A.1+A.2.1, for each research unit)
- item C: cost of equipment, tools and software products
- item D: cost of consulting and similar services
- item E: other operating costs

PART B

B.1

---

1. State of the art

NONINTERFERENCE

Noninterference is an information flow security property aiming to protect information confidentiality by guaranteeing that high level, sensitive information never flows to low level, unauthorized users due to covert channels or weaknesses in cryptographic algorithms. Noninterference for deterministic systems was introduced in [GM82] and then applied to programming languages [SM03], trace models [McL94], cryptographic protocols [ABF18], process calculi [FG00, HR02], timed models [FGM03], and probabilistic and stochastic models [AB09].

Conditional noninterference, which admits flows from a high security level to a low one through a controlled or trusted part supporting some form of downgrading, was first addressed in [GM84]. Downgrading was then modelled in [BPR04] in the context of CCS [Mil89]. Conditional and partial information flows were investigated in [RS01] in the CSP setting [BHR84], where flows are admitted from the high level to a trusted part and from the latter to the low level, provided that the trusted part takes care of controlling them.

Noninterference for systems expressed as Markovian process algebra terms was studied in [HPR18] through a quantitative extension named persistent stochastic noninterference (PSNI). Assuming that an observer can see any execution path with its delays, timing aspects such as response time and system throughput may produce information leakage. A generalization of PSNI called D_PSNI was presented in [HMPR19], which allows information to flow from a higher to a lower security level through a downgrader. Both PSNI and D_PSNI can be decided in polynomial time through generalizations of lumpability algorithms [HPR18, HMPR19].

REVERSIBILITY

Irreversible computations cause heat dissipation into circuits [Lan61], hence low energy consumption can be achieved by supporting reversibility [Ben73]. Reversible computing has many applications ranging from biochemical reactions [PUY13] and parallel discrete-event simulation [SOBJ18] to robotics [LES18], fault-tolerant distributed systems [VS18], and program debugging [GLM14]. In a reversible system, featuring forward and backward computations, one can backtrack by starting from the last action. In a concurrent system the last action is hard to identify as there are several interacting processes. The only viable option is causal consistent reversibility: an action can be undone only if all of its consequences have been undone already.

In concurrency theory we have two process algebraic approaches to reason about reversible systems, both based on CCS [Mil89]. The former, RCCS [DK04], extends the syntax by attaching stack-based memories to processes so as to record all the executed actions. The latter, CCSK [PU07], modifies the operational semantics in order to generate labeled transition systems that are causal consistent reversible. The two approaches are equivalent in terms of labeled transition system isomorphism [LMM19].

A different notion known as time reversibility [Kel79] was developed in the performance evaluation field. A stochastic process is time reversible if its behavior remains the same when the direction of time is reversed. This notion, instrumental to devise efficient analysis methods, was also studied in a Markovian process algebra setting [Har03, MR15] and recently blended with causal consistent reversibility [BM20].

BLOCKCHAIN

Blockchain technology [ZXDCW17] enables secure transactions among untrusted parties in a decentralized and disintermediated environment. A blockchain is a distributed data structure composed of blocks linked

together through cryptography, each containing the hash value of the previous block, a timestamp, and transaction data. Once stored, data cannot be altered or removed from the blockchain. This immutability property certifies that transaction data residing in the blockchain are tamper-proof.

A blockchain results in an append-only distributed ledger that records transactions in a verifiable and permanent manner. The parties form a peer-to-peer communication network adhering to a consensus protocol for block validation. Usually a blockchain is public, like for virtual currencies [N08], meaning that the ledger is accessible by anyone without specific read, write, or validate permissions. Transaction validation is accomplished algorithmically, with no central authority.

Data immutability guarantees that everyone can trust the blockchain, but may be in contrast with regulations enforcing transaction cancellation or data amendment. In these cases, as well as in the case of central bank digital currency [BL18], a private blockchain may be more appropriate, as it can be accessed only by authorized people and is governed by a designated person, enterprise, or authority. Methods for reversing transactions are thus needed in a private blockchain, and unauthorized information flows from its governance to the various parties must be avoided.

---

2. Detailed description of the project: methodologies, objectives and results that the project aims to achieve and its interest for the advancement of knowledge, as well as methods of dissemination of the results achieved

PREAMBLE

Nowadays computing systems are large scale, physically distributed services, possibly including various kinds of data collection sensors. They are used for communication purposes, performing transactions, and providing information to efficiently manage assets, resources, and operations or suitably drive the adoption of context-dependent decisions autonomously. These smart systems are inherently pervasive, interact extensively with their environment, and support a huge number of users. The design, implementation, and deployment of these systems pose new challenges whose complexity can be managed only by resorting to a model-based approach in the early stages, so as to take advantage of the benefits of formal and semi-formal methods in terms of system description and property prediction. A holistic view is also necessary as the trustworthiness of such systems encompasses several aspects like safety, security, integrity, efficiency, availability, resilience, and ease of use, which need to be addressed as a whole. Last but not least, compliance with regulations must be ensured; think, e.g., of personal data protection.

Among the existing distributed platforms, in the past ten years blockchain technology has witnessed an increasingly widespread adoption, especially to avoid the double spending problem in the setting of virtual currency platforms like Bitcoin, Ethereum, and Ripple. A blockchain is an append-only distributed ledger that permanently records transactions taking place among untrusted parties in a decentralized and disintermediated environment. The parties form a peer-to-peer asynchronous communication network adhering to a cryptography-based consensus protocol for validating blocks of transactions in the chain. Users are free to enter, leave, and join again the network at any time and validate transactions algorithmically, with no central authority, based on a computationally expensive mechanism that discourages potential attackers. Despite their success, blockchains are not exempt from shortcomings arising from misuse and immutability.

Decentralization and freedom of access have produced some undesired consequences. Firstly, since anyone can read and write the distributed ledger, blockchain transactions have fueled black market trading. Secondly, since the consensus protocol is energy consuming, the majority of users operate in countries with cheap electricity, leading to network centralization and the possibility of collusion, in addition to making the network vulnerable to changes in policies on electricity subsidies. Both of these trends have determined an increasing interest in private blockchains, which could ultimately give businesses a greater degree of control. Different from a public, unpermissioned blockchain, a private one can be accessed only by people having the permission of reading the ledger, submitting transactions, and/or validating transactions, with the network being governed by a designated person, enterprise, or authority. Since the involved parties are no longer peers, but are differentiated according to their permissions, in a private blockchain it is of paramount importance to avoid unauthorized information flows from its governance to the various parties interested in performing transactions.

A pillar of blockchain technology is data immutability. Once stored, data cannot be altered or removed from the blockchain. This property certifies that data residing in a public blockchain are tamper-proof, thus creating a digital environment trusted by all parties despite the absence of a central authority certifying user identity and transaction validity. Unfortunately, data immutability may conflict with regulations and the only way out is allowing for some degree of mutability [PCAP21, Gar20]. One example is the right to be forgotten, introduced within the EU in 2016 by the General Data Protection Regulation (GDPR) after the adoption in 2014 of the Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS). Other examples are transactions performed as a consequence of digital identity theft or in spite of contract nullity or infringement. In all these cases, the effects of the considered illegal transactions have to be removed from the blockchain. Again, this seems to be more feasible in a private blockchain rather than in a public one, as in the former it is likely that the owner is endowed with mechanisms for deeming a transaction as reversible due to the permission-based accessibility of the private blockchain. After all, the idea of reversibility has already been considered for virtual currencies, leading for instance to Reversecoin [Men14], where vault accounts are additionally available with a configurable timeout such that transactions can be reversed before the timeout expires while remaining visible in the ledger, and reversible Initial Coin Offerings [Vog20], based on smart contracts mimicking fund raising in the real world.

The rapid pace of innovations in payment technology due to virtual currencies could threaten monetary sovereignty and undermine financial stability by accelerating currency substitution. Scenarios in which central banks do not produce any form of digital currency may be associated with a number of salient risks, including loss of monetary control and greater susceptibility to severe economic downturns. As a consequence, many of these banks are moving expeditiously towards exploring issuance, distribution, and transfer of what is called central bank digital currency (CBDC) [BL18], which combines the digital nature of deposits with the peer-to-peer use of cash. Just like paper currency and coins, CBDC would be fixed in nominal terms, universally accessible, and valid as legal tender for all public and private transactions. Therefore, CBDC is essentially different from the various forms of virtual currency created by private entities, whose market prices have exhibited very sharp fluctuations in recent years, and should support a much higher number of transactions per unit of time, comparable to that of debit and credit cards. In addition to reducing costs associated with issuing and managing physical cash and hopefully enhancing financial digitalization and inclusion, a widespread use of CBDC would be helpful in discouraging tax evasion, money laundering, and other illegal activities. Regardless of CBDC being token-based or account-based to serve as a practically costless medium of exchange, as well as interest-bearing to provide a secure store of value in line with other risk-free assets such as short-term government securities, private blockchains are expected to play a pivotal role as an enabling technology. They would thus result in a critical digital infrastructure, to which formal methods should be applied to develop models useful for the early assessment of correctness, security, and performance issues.

OBJECTIVES AND METHODOLOGIES

The objective of the NiRvAna project is to advance the state of the art in the fields of computer security, especially noninterference analysis ensuring that sensitive information never flows from a high level to a low level of security, as well as reversible computing, intended as a correct mechanism for undoing transactions in a distributed system, and then apply the resulting techniques to private blockchains, with a special emphasis on CBDC. Following a holistic view, in noninterference and reversibility analyses we will address not only functional features, but also quantitative aspects.

Process algebra [Mil89, BHR84] will be adopted as a working formalism common to all the research units involved in the project. On the one hand, this will allow us to benefit from an abstract modeling language, where distributed system descriptions can be built compositionally by means of a parsimonious set of behavioral operators such as action prefix, alternative composition, and parallel composition. Process terms are then automatically mapped via operational semantic rules to state-transition graphs called labeled transition systems, where states represent process terms derived from the initial one and transitions are labeled with their corresponding actions. On the other hand, we will make use of behavioral equivalences, which permit relating process algebraic models that, despite their syntactical differences, represent the same behavior in that they cannot be distinguished by an external observer. Behavioral equivalences are also useful to reduce the size of the state-transition graph underlying a system description while preserving specific properties to be assessed later, and come equipped with equational and logical characterizations helpful to explain why two models are equivalent or not. Among the various approaches to the definition of these equivalences, we will focus on the well established notion of bisimilarity [Mil89], which amounts to the ability of mimicking each other's behavior stepwise.

Quantitative aspects will be addressed by working with Markovian process algebra [Hil96], in which every action of a process term is extended with a positive real number expressing the rate of the exponential distribution quantifying the duration of the action. The operational semantic rules of this enhanced modeling language produce labeled transition systems in which every transition is thus labeled with an action and its rate. As a consequence, the underlying performance model naturally is a stochastic process in the form of a continuous-time Markov chain (CTMC) [KS60], possibly enriched with state and transition rewards that formalize quantitative properties of interest [BB03]. Throughout the project, we will use Performance Evaluation Process Algebra (PEPA) [Hil96] as a modeling language, possibly developing extensions or variants of it based on the project needs, along with the PEPA Eclipse plug-in developed at the University of Edinburgh. The latter is a verification tool, in which we plan to implement our new techniques, that supports steady-state analysis [Ste94], ordinary differential equation (ODE) analysis [TGH12], and abstraction and model checking of properties expressed in Continuous Stochastic Logic (CSL) [BHHK03]. We mention that the PEPA language is also accepted by other tools, which we will use in case of need, including the Moebius modeling framework from the University of Illinois at Urbana-Champaign, the PRISM probabilistic model checker from the Universities of Birmingham and Oxford, and the CADP toolbox from INRIA Rhone-Alpes in Grenoble.

Software tool websites:
- http://www.dcs.ed.ac.uk/pepa/tools/plugin/
- https://www.mobius.illinois.edu/
- https://www.prismmodelchecker.org/
- http://cadp.inria.fr/

EXPECTED ADVANCES IN NONINTERFERENCE ANALYSIS

In the last decades, security of information systems has become a crucial topic of research. Despite numerous definitions of security have been proposed, very few results take into account the time behaviour of systems. It is well known that from the observation of the response times of a system, malicious observers can infer characteristics that may help an attack to succeed. In [HPR18], we provided results to cover this gap by specifying systems in PEPA, which allowed us to model quantitative system properties, and by introducing the notion of persistent stochastic noninterference (PSNI), which is a quantitative extension of the noninterference property widely used to secure systems from a functional point of view in terms of absence of covert channels.

Let us consider a system S that performs some actions that are intended to be confidential and some others that are observable by an external, possibly malicious, user. Roughly speaking, S is secure if no external observer is able to distinguish the behaviour of S performing confidential, secret activities from the behaviour of S when prevented from executing those activities. In [HPR18], the definition assumes also that the observer is able to measure the timing properties of S. In particular, we considered the strictest situation in terms of security requirements: the observer can see any observable execution path with its delays, i.e., the transient behaviour of S, and then study correlation properties, averages, etc. Moreover, the observer can study the functional and quantitative behaviour of S for an arbitrarily long amount of time.

In order to capture the timing properties of a system, the notion of observation that we considered, named lumpable bisimilarity, is based on the concept of lumpability for the underlying CTMC [KS60]. Lumpable bisimilarity requires strict conditions on the outgoing rates of process terms, in particular two process terms are considered lumpably bisimilar if the transition rates from these terms to any equivalence class are the same, except for the case of invisible transitions leading to the equivalence class of the two terms. Moreover, it allows one to efficiently compute the exact values of performance indices when the model is actually lumpable.

It is well known that not all CTMCs are lumpable, if we exclude the trivial aggregation reducing a chain to a single state. In fact, only a small percentage of CTMCs arising in real-life applications is expected to be non-trivially lumpable. Therefore, in real-world situations it may be difficult to find a system that satisfies all the requirements of PSNI. One of the goals of this project is that of facing the problem of relaxing the conditions of lumpability while allowing one to derive exact or slightly approximated stationary performance indices for the original process. In particular, we aim at introducing notions of approximated lumpability and defining new security properties for stochastic processes based on such novel concepts of approximated lumpability. We then propose to relax the conditions underlying the definition of PSNI. A first effort in this direction can be found in [MPR19], where the notion of proportional lumpability was introduced.

Moreover, we plan to extend the notion of PSNI to allow mechanisms for downgrading or declassifying information such as information filters and channel control. Furthemore, horizontal and vertical refinements will be studied to improve the development of secure models and, eventually, correct them.

In [AMPR18], we implemented the lumpability notion at the basis of PSNI within the PEPA Eclipse plug-in. We intend to enrich the plug-in input language in order to allow the specification of multi-level systems. PEPA already accepts any system defined in terms of finite action-labeled CTMCs, but at the moment there is no distinction between high and low level actions. Such an extension will easily allow us to encode an algorithm for PSNI. Subsequently, we will also include implementations of the new approximated security notions we are going to define within this project. Moreover, we will evaluate the opportunity of enriching the language with specific application-driven operators that could simplify the modeling process. Finally, again with the aim of easing the modeling phase and enlarging the community of users of our security notions, we will provide scripts

for the translation into PEPA of systems described within different formalisms.

Further bibliography:
[AMPR18] Alzetta Marin Piazza Rossi; Lumping-Based Equivalences in Markovian Automata: Algorithms and Applications to Product-Form Analyses; Information and Computation 260:99-125
[MPR19] Marin Piazza Rossi; Proportional Lumpability; FORMATS, LNCS 11750:265-281

EXPECTED ADVANCES IN REVERSIBILITY ANALYSIS

Recently the notions of causal consistent reversibility and time reversibility were jointly addressed in a Markovian process algebra setting [BM20]. The aim was to bridge the gap between those two notions of reversibility for a twofold reason. On the one hand, quantitative aspects had been disregarded in the context of causal consistent reversibility. On the other hand, the theory of time reversibility had been applied to concurrent systems without explicitly taking causality into account.

Following the approach of [PU07], forward and backward operational semantic rules were provided in [BM20] that result in a causal consistent reversible Markovian process calculus. The novelty is that this was established by borrowing the notion of concurrent transitions from the alternative approach of [DK04]. After observing that the CTMC underlying the calculus is stationary, it was shown that time reversibility can be achieved by using, in the operational semantic rules, backward rates equal to the corresponding forward rates. Guaranteeing time reversibility by construction is quite different from previous works in the same setting like [Har03, MR15], where time reversibility is investigated a posteriori. It was also adapted from [MR15] a product form result that enables the efficient calculation of performance measures.

Further steps are needed in the quest towards the integration of causal consistent reversibility and time reversibility. For instance, it is important to investigate other conditions, in addition to the one relying on the equality of forward and backward rates, under which time reversibility can be achieved by construction, hopefully in conjunction with new product form results. Another issue is that, in the presence of recursion, the use of communication keys typical of the approach of [PU07] produces an infinite state space in situations in which traditional process calculi yield a finite one. This calls for a careful design of the semantic rules for parallel composition and communications, leading to a mechanism lighter than communications keys to keep track of past actions. We also plan to implement a reversible variant of PEPA in the Eclipse plug-in based on the achieved results.

Most importantly, behavioral equivalences have to be studied for reversible Markovian process calculi. In the nondeterministic setting, when considering both the forward direction of computation and the backward one for reversibility purposes, bisimilarity simultaneously takes both directions into account by examining not only outgoing transitions, but also incoming ones. In this back-and-forth mode, causality is always respected whereas this is not necessarily the case for history in the presence of concurrency, in the sense that one may proceed forward along a certain path and then backward along a different path in which the actions of the various processes are interleaved in a different way. The choice made in [DMV90] was that of respecting history too, hence back-and-forth bisimilarity was defined on runs rather than states and shown to coincide with the forward bisimilarity of [Mil89]. In contrast, in [PU07] history may not be respected, hence the resulting back-and-forth bisimilarity on states does not satisfy the expansion law of [Mil89] and essentially boils down to a variant of bisimilarity for truly concurrent models as later shown in [PU12].

In Markov chain theory, the forward direction and the backward one are instead considered separately. The forward direction, which is based on outgoing transitions, yields ordinary lumpability [KS60], which coincides with the Markovian bisimilarity of [Hil96]. Ordinary lumpability is an aggregation such that the steady-state (resp. transient) probability of each aggregate state is the sum of the steady-state (resp. transient) probabilities of the original states belonging to the aggregate one. The backward direction, which is based on incoming transitions, yields exact lumpability [Sch84], which additionally ensures, with respect to ordinary lumpability, that all the original states belonging to an aggregate state possess the same steady-state (resp. transient) probability. The variant of Markovian bisimilarity induced by exact lumpability was studied in [Buc99] with respect to compositionality properties of stochastic automata and in [SD06] with respect to the preservation of CSL formulas for model checking purposes.

On the one hand, it is interesting to understand to what extent the back-and-forth mode of nondeterministic process calculi can be reconciled with the separate view of Markov chain theory. For example, it should be investigated whether the approach of [DMV90] scales to Markovian process calculi, i.e., whether the resulting back-and-forth bisimilarity coincides with the Markovian bisimilarity of [Hil96]. On the other hand, while compositionality properties and equational and logical characterizations are well known for the Markovian bisimilarity of [Hil96], this is not the case for the Markovian bisimilarity induced by exact lumpability. Apart from the fact that the two bisimilarities are incomparable in terms of distinguishing power [SD06], very little is known about the latter. We will thus study alternative views of the Markovian bisimilarity induced by exact lumpability, including a sound and complete axiomatization as well as a modal logic characterization. Again, we plan to implement the obtained results in the PEPA Eclipse plug-in.

Further bibliography:
[Buc99] Buchholz; Exact Performance Equivalence: An Equivalence Relation for Stochastic Automata; Theoretical Computer Science 215:263-287
[Sch84] Schweitzer; Aggregation Methods for Large Markov Chains; CPR, North Holland 275-286
[SD06] Sproston Donatelli; Backward Bisimulation in Markov Chain Model Checking; IEEE Trans. Software Engineering 32:531-546

EXPECTED APPLICATIONS TO PRIVATE BLOCKCHAINS

The aforementioned expected advances will lead to a reversible Markovian process algebra equipped with stochastic noninterference techniques that we will apply to the study of private blockchains. We will start by developing models of various aspects of blockchains in general, such as distributed ledgers, consensus protocols, and peer-to-peer asynchronous networks. In doing this, we will consider performance aspects too, by taking inspiration from some recent works in our Markovian setting like [KT17, KRS18, BDGLMV20]. Then we will focus on private blockchains, in which noninterference and reversibility analyses play a role due to the presence of users with different permissions, and hence different security levels, as well as the necessity of reversing transactions in certain situations, for regulation compliance. Special attention will be paid to CBDC, for which we are already consulting the relevant literature including working papers and reports of the International Monetary Fund, the World Economic Forum, and central banks.

We plan to develop a complete compositional model of a private blockchain written in a reversible variant of PEPA, whose correctness, security, and performance properties will be analyzed with our extension of the PEPA Eclipse plug-in. We will then work together with BAX, a firm located in the province of Pesaro and Urbino operating in the field of information and communication technology, to implement a prototype of our verified model of private blockchain. BAX is involved in the regional project MIRACLE (Marche Innovation and Research fAcilities for Connected and sustainable Living Environments) funded by Regione Marche and this will allow us to

exploit the computing facilities of a dedicated server farm.

Further bibliography:
[BDGLMV20] Bistarelli De-Nicola Galletta Laneve Mercanti Veschetti; Stochastic Modelling and Analysis of Bitcoin; technical report
[KT17] Kamil Thomas; Modelling and Analysis of Commit Protocols with PEPA; EPEW, LNCS 10497:266-281
[KRS18] Kiffer Rajaraman Shelat; A Better Method to Analyze Blockchain Consistency; CCS, ACM 729-744

METHODS OF DISSEMINATION

The results achieved within the NiRvAna project will be submitted to international conferences (e.g., CONCUR, FOSSACS, TACAS, FORTE, RC, QEST, FORMATS usually taking place in Europe and North America) and journals (e.g., Information and Computation, Theoretical Computer Science, Logical Methods in Computer Science, Performance Evaluation, Computer Security) relevant to the field. Preference will be given to publication venues that offer open access or creative-common copyright licenses. A public website of the project, possibly equipped with social channels, will collect all the information about milestones, publications, case studies, software tools, and presentations. Seminars and events organized during the project will also be advertised on the website and, when possible, broadcast and maintained. We hope that the scientific achievements of our project will lay the foundations for enlarging our international network of collaborations and preparing a EU-funded proposal. We plan to organize not only academic meetings, but also conferences and panel discussions with industrial and institutional stakeholders in order to raise awareness on the topic in the society.

3. Project development, with identification of the role of each research unit, with regards to related modalities of integration and collaboration

The development of the NiRvAna project will be structured according to the 5 work packages illustrated in the following. The research unit of the PI will be in charge of supervising the execution and the timing of the 13 tasks constituting the 5 work packages. In addition to virtual project meetings whenever necessary, four physical plenary meetings will take place, at which other researchers interested in the field as well as industrial and institutional stakeholders will be invited. The kick-off meeting, to be held in Urbino at month 1, will focus on the state of the art at the time of the approval of the project proposal. The first mid-term meeting, to be held in Venice at month 12, and the second mid-term meeting, to be held in Udine at month 24, will check the level of achievement of the expected results. The closing meeting will be organized in Urbino at month 36. The research unit of the PI will create within month 2, and subsequently maintain, a public website dedicated to the project. It will also take care of coordinating all the dissemination activities described at the end of the previous section of the proposal.

WP1 - MARKOVIAN BEHAVIORAL EQUIVALENCES

This work package, led by Sabina Rossi and Marco Bernardo, is concerned with the advances in behavioral equivalences, inspired by the concepts of approximated, ordinary, and exact lumpability, that are necessary to conduct noninterference and reversibility analyses in a CTMC-based setting. All the three research units will be involved in this work package and cooperate in the execution of the following tasks:

* T1.1 - Approximated lumpability-based equivalence (months 1-18)
We will explore how to relax the conditions at the basis of lumpability while allowing one to derive exact or slightly approximated stationary performance indices for the original process. In particular, we aim at introducing a notion of approximated lumpability. A first effort in this direction can be found in [MPR19], where proportional lumpability was introduced.

* T1.2 - Back-and-forth Markovian bisimilarity (months 1-12)
We will apply to our Markovian setting the approach of defining back-and-forth bisimilarity on runs rather than states so as to preserve history when going backward [DMV90] and then investigate whether the resulting behavioral equivalence coincides with the Markovian bisimilarity of [Hil96].

* T1.3 - Exact-lumpability-based Markovian bisimilarity (months 1-12)
We will study the properties of the Markovian bisimilarity induced by exact lumpability, which considers incoming transitions rather than outgoing ones, in terms of discriminating power and compositionality with respect to typical process algebraic operators, along with a sound and complete axiomatization and a modal logic characterization.

WP2 - STOCHASTIC NONINTERFERENCE ANALYSIS

This work package, led by Sabina Rossi and Carla Piazza, is concerned with the advances in noninterference analysis that will stem from considering, for systems with users at different security levels, also their time behavior. The research units of UniVe and UniUd will concentrate on this work package given their expertise in the field, without excluding collaborations with the other research unit. The specific tasks are as follows:

* T2.1 - Approximated stochastic noninterference (months 13-24)
We plan to define new security properties for stochastic processes based on the novel concepts of approximated lumpability of WP1. We will then relax the conditions underlying the definition of PSNI in order to be applicable to security issues for a wide class of processes representing real-world applications, in particular private blockchains.

* T2.2 - Downgrading and refinements (months 13-24)
In order to further relax the conditions of PSNI, we will study how to include in our definitions mechanisms for downgrading or declassifying information such as information filters and channel control. In particular, we will define a notion of approximated delimited PSNI. Moreover, we will investigate the preservation of stochastic noninterference under both horizontal and vertical refinements, which are useful techniques for model correction and development.

WP3 - INTEGRATED REVERSIBILITY ANALYSIS

This work package, led by Claudio Antares Mezzina, is about the advances in reversibility analysis that will arise from the combination of causal consistent reversibility typical of distributed systems and time reversibility of Markov chain theory. The research unit of UniUrb will focus on this work package due to its expertise in the field, not excluding collaborations with the other two research units. Here are the detailed tasks:

* T3.1 - Time reversibility by construction (months 1-18)
We will look for other conditions, in addition to the one relying on the equality of forward and backward rates in the reversible Markovian process calculus of [BM20], under which time reversibility is achieved, hopefully in conjunction with new product form results.

* T3.2 - Keeping the state space finite (months 1-18)
We will address the generation of an infinite state space in [BM20] in situations in which forward-only process calculi yield a finite one, by revisiting the interplay between recursion and parallel composition through a mechanism lighter than the communications keys used to keep track of past actions according to the adoption of the technique of [PU07].

WP4 - SOFTWARE TOOL IMPLEMENTATION

This work package, led by Carla Piazza and Claudio Antares Mezzina, is about the implementation in the PEPA Eclipse plug-in, and possibly in other tools supporting PEPA, of the modeling languages and analysis techniques of the previous work packages. All the three research units will be involved in this work package and cooperate to carry out the following tasks:

* T4.1 - Extensions of the modeling language (months 13-24)
We will enrich the syntax of PEPA in the Eclipse plug-in to specify the security levels of actions, so as to enable noninterference analysis, and subsequently extend its operational semantics with backward rules, in order to support reversibility by construction as of WP3.

* T4.2 - Implementation of behavioral equivalences (months 13-24)
We will then implement the Markovian behavioral equivalences studied in WP1 by means of the corresponding partition refinement algorithms, along with the production of diagnostic information useful to explain why two systems are not equivalent, as well as the related CTMC-level aggregations.

* T4.3 - Implementation of noninterference properties (months 25-30)
We will finally implement the stochastic noninterference techniques developed in WP2 on the basis of the aforementioned implementation of our Markovian behavioral equivalences.

WP5 - APPLICATIONS TO PRIVATE BLOCKCHAINS

This work package, led by Marco Bernardo, has to do with the application to private blockchains of the modeling languages and analysis techniques implemented in WP4. All the three research units will be involved in this work package and cooperate towards the accomplishment of the following tasks:

* T5.1 - Compositional model of a private blockchain (months 7-24)
We will develop Markovian process algebra models of various aspects of blockchains such as distributed ledgers, consensus protocols, and peer-to-peer asynchronous networks as a stepping stone to get a complete compositional model of a private blockchain written in a reversible variant of PEPA.

* T5.2 - Verification of the private blockchain model (months 25-36)
We will then assess correctness, security, and performance properties of the private blockchain model by using the PEPA Eclipse plug-in extended with our techniques for stochastic noninterference analysis as well as causal consistent reversibility integrated with time reversibility.

* T5.3 - Implementation of a prototype of the verified model (months 25-36)
We will finally build together with BAX a prototype of the verified model of private blockchain in the server farm made available within the MIRACLE project funded by Regione Marche.

4. Possible application potentialities and scientific and/or technological and/or social and/or economic impact, with indications of the possible use of research infrastructures

The focus of the NiRvAna project is in the ICT area, in particular distributed computing, which acts as a major enabling technology for large-scale digital services. The planned research outcomes that will be pursued in this project are specifically relevant for blockchain technology, which is experiencing an increasing interest not only for its primary application to virtual currencies, but also for its more recent employment within manufacturing industries, logistics, agriculture, health care, real estate, smart communities, and personal identity security. The socio-economic impact of this technology is ever growing, especially in the case of permissioned, private blockchains. Therefore, we expect the results of our project to raise awareness in the society on the importance of designing efficient private blockchains that are free of undesired information flows from the blockchain governance to its users and, unlike public ones, are able to reverse transactions whenever this is required by regulations. Think for instance of central banks, which can no longer take a passive and inertial approach to adopting digital currency as witnessed by a large number of reports prepared by financial and monetary institutions, and the fact that errors, data breaches, and poor performance in CBDC platforms may have economical and social consequences hard to estimate.

From a scientific viewpoint, our project will advance the state of the art in formal methods in computer science for noninterference and reversibility modeling and analysis by taking quantitative aspects into account too. More specifically, on the one hand our techniques will allow one to investigate the absence of information leakage from a high security level to a low one due to covert channels that may be based not only on functional features, but also on performance aspects. On the other hand, our combination of causal consistent reversibility typical of distributed systems with time reversibility of Markov chain theory will allow one to build models reversible by construction, in which transactions can be undone in a way that timely brings the system in a previous consistent state. At the foundational level, Markovian behavioral equivalences inspired by the notions of approximated, ordinary, and exact lumpability will be better understood. At the application level, software tools developed in the concurrency, security, and performance communities will be extended accordingly along with their modeling languages and verification capabilities, hopefully fostering collaborations with the research groups that released those tools, so as to enable a more accurate property prediction of complex systems.

In the third year of our activities we plan to use the research infrastructure of the MIRACLE project funded by Regione Marche. This project involves a number of small and medium enterprises located in the region and aims at establishing innovation and research facilities for connected and sustainable living environments. Together with BAX, an ICT company in the province of Pesaro and Urbino, we will implement a prototype of our verified model of private blockchain in the server farm made available within the MIRACLE project. This will be an important occasion for experimenting with our techniques and seeing them at work.

5. Financial aspects: costs and funding for each research unit

nº		Total cost (euro)	Co-funding (item A.1) (euro)	MUR funding (other items) (euro)
1.	BERNARDO Marco	291.373	112.108	179.265
2.	ROSSI Sabina	248.552	89.720	158.832
3.	PIAZZA Carla	242.747	86.092	156.655
	Total	**782.672**	**287.920**	**494.752**

6. Bibliography

[ABF18] Abadi Blanchet Fournet; The Applied Pi Calculus: Mobile Values, New Names, and Secure Communication; J. ACM 65:1-41
[AB09] Aldini Bernardo; A General Framework for Nondeterministic, Probabilistic, and Stochastic Noninterference; ARSPA/WITS, LNCS 5511:18-33
[BHHK03] Baier Haverkort Hermanns Katoen; Model-Checking Algorithms for Continuous-Time Markov Chains; IEEE Trans. Software Engineering 29:524-541, 2003.
[Ben73] Bennett; Logical Reversibility of Computations; IBM J. Research and Development 17:525-532
[BB03] Bernardo Bravetti; Performance Measure Sensitive Congruences for Markovian Process Algebras; Theoretical Computer Science 290:117-160
[BM20] Bernardo Mezzina; Towards Bridging Time and Causal Reversibility; FORTE, LNCS 12136:22-38
[BL18] Bordo Levin; Central Bank Digital Currency and The Future of Monetary Policy; Monetary Policy and Payments 3:143-178
[BPR04] Bossi Piazza Rossi; Modelling Downgrading in Information Flow Security; CSFW, IEEE 187-201
[BHR84] Brookes Hoare Roscoe; A Theory of Communicating Sequential Processes; J. ACM 31:560-599
[DK04] Danos Krivine; Reversible Communicating Systems; CONCUR, LNCS 3170:292-307
[DMV90] De-Nicola Montanari Vaandrager; Back and Forth Bisimulations; CONCUR, LNCS 458:152-165
[FG00] Focardi Gorrieri; Classification of Security Properties (Part I: Information Flow); FOSAD, LNCS 2171:331-396
[FGM03] Focardi Gorrieri Martinelli; Real-Time Information Flow Analysis; Selected Areas in Communications 21:20-35
[Gar20] Garcia-Teruel; Legal Challenges and Opportunities of Blockchain Technology in the Real Estate Sector; Property, Planning and Environmental Law 12:129-145
[GLM14] Giachino Lanese Mezzina; Causal-Consistent Reversible Debugging; FASE, LNCS 8411:370-384
[GM82] Goguen Meseguer; Security Policy and Security Models; SSP, IEEE 11-20
[GM84] Goguen Meseguer; Unwinding and Inference Control; SSP, IEEE 75-86
[Har03] Harrison; Turning Back Time in Markovian Process Algebra; Theoretical Computer Science 290:1947-1986
[HR02] Hennessy Riely; Information Flow vs. Resource Access in the Asynchronous Pi-Calculus; ACM Trans. Programming Languages and Systems 24:566-591
[Hil96] Hillston; A Compositional Approach to Performance Modelling; Cambridge University Press
[HMPR19] Hillston Marin Piazza Rossi; Delimited Persistent Stochastic Non-Interference; VALUETOOLS, ACM 135-142
[HPR18] Hillston Piazza Rossi; Persistent Stochastic Non-Interference; EXPRESS/SOS, EPTCS 276:53-68
[Kel79] Kelly; Reversibility and Stochastic Networks; Wiley

[KS60] Kemeny Snell; Finite Markov Chains; Van Nostrand
[Lan61] Landauer; Irreversibility and Heat Generated in the Computing Process; IBM J. Research and Development 5:183-191
[LMM19] Lanese Medic Mezzina; Static versus Dynamic Reversibility in CCS; Acta Informatica
[LES18] Laursen Ellekilde Schultz; Modelling Reversible Execution of Robotic Assembly; Robotica 36:625-654
[MR15] Marin Rossi; Quantitative Analysis of Concurrent Reversible Computations; FORMATS, LNCS 9268:206-221
[McL94] McLean; A General Theory of Composition for Trace Sets Closed under Selective Interleaving Functions; SSP, IEEE 79-93
[Men14] Menezes; Reversecoin - The World's First Cryptocurrency with Reversible Transactions; https://bitcoinist.com/reversecoin-worlds-first-cryptocurrency-reversible-transactions/
[Mil89] Milner; Communication and Concurrency; Prentice Hall
[N08] Nakamoto; Bitcoin: A Peer-to-Peer Electronic Cash System; https://bitcoin.org/bitcoin.pdf
[PU07] Phillips Ulidowski; Reversing Algebraic Process Calculi; Logic and Algebraic Programming 73:70-96
[PU12] Phillips Ulidowski; A Hierarchy of Reverse Bisimulations on Stable Configuration Structures; Mathematical Structures in Computer Science 22:333-372
[PUY13] Phillips Ulidowski, Yuen; A Reversible Process Calculus and the Modelling of the ERK Signalling Pathway; RC, LNCS 7581:218-232
[PCAP21] Politou Casino Alepis Patsakis; Blockchain Mutability: Challenges and Proposed Solutions; IEEE Trans. Emerging Topics in Computing
[RS01] Ryan Schneider; Process Algebra and Non-Interference; Computer Security 9:75-103
[SM03] Sabelfeld Myers; Language-Based Information-Flow Security; Selected Areas in Communication 21:5-19
[SOJB18] Schordan Oppelstrup Jefferson Barnes; Generation of Reversible C++ Code for Optimistic Parallel Discrete Event Simulation; New Generation Computing 36:257-280
[Ste94] Stewart; Introduction to the Numerical Solution of Markov Chains; Princeton University Press
[TGH12] Tribastone Gilmore Hillston; Scalable Differential Analysis of Process Algebra Models; IEEE Trans. Software Engineering 38:205-219
[VS18] Vassor Stefani; Checkpoint/Rollback vs. Causally-Consistent Reversibility; RC, LNCS 11106:286-303
[Vog20] Vogelsteller; rICO - The Reversible ICO; https://medium.com/lukso/rico-the-reversible-ico-5392bf64318b
[ZXDCW17] Zheng Xie Dai Chen Wang; An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends; BD, IEEE 557-564

B.2

1. Scientific Curriculum of the Principal Investigator

Marco Bernardo was born in Bologna in 1970. He received a Laurea in Computer Science in 1994 and a PhD in Computer Science in 1999, from the University of Bologna. In 1997 he was a visiting PhD student at the North Carolina State University. After a short period as research assistant in computer science at the University of Bologna, from 1999 to 2001 he was a tenured researcher in computer science at the University of Torino and from 2001 to 2018 an associate professor of computer science at the University of Urbino. Since 2018 he is a full professor of computer science at the University of Urbino.

He authored more than 120 scientific publications in the field of theoretical computer science, in particular semantics of programming languages and verification of software correctness, among which the book "A Process Algebraic Approach to Software Architecture Design" published by Springer in 2010. His PhD thesis "Theory and Application of Extended Markovian Process Algebra" received a prize in 1999 by the Italian Chapter of the European Association for Theoretical Computer Science (EATCS). His paper "A Uniform Framework for Modeling Nondeterministic, Probabilistic, Stochastic, or Mixed Processes and Their Behavioral Equivalences" was recognized in 2016 as highly cited research by the scientific journal Information and Computation published by Elsevier. He was a member of the scientific committee of numerous international conferences and played the role of principal investigator in the PRIN national research project "Performability-Aware Computing: Logics, Models, and Languages (PaCo)" from 2008 to 2010 and workpackage leader in the PRIN national research project "Compositionality, Interaction, Negotiation and Autonomicity in the Future ICT Society (CINA)" from 2013 to 2016.

His current H-index is 19 according to Scopus, where 108 publications and 1188 citations are recorded.

Since 2001 he taught courses on Procedural Programming, Logic Programming, Functional Programming, Algorithms and Data Structures in the Laurea Programme in Applied Informatics and since 2011 he was a member of the Board of the PhD Programme currently called Research Methods in Science and Technology, at the University of Urbino. From 2001 to 2016 he organized at the Congress Center of Bertinoro the series of PhD summer schools "International School on Formal Methods for the Design of Computer, Communication and Software Systems (SFM)". From 2012 to 2014 he was a visiting scholar and then a visiting professor at IMT Lucca.

At the University of Urbino he was appointed Chair of the Laurea Programme in Applied Informatics (2002-2003, 2003-2006, 2006-2007, 2011-2013), Director of the Master in Home and Building Automation (2006-2007), Rector's Delegate for Technological Innovation (2014-2020), Deputy Director of the Integrated Center for Teaching Services and E-Learning (2015-2018, 2018-2021), and member of the Administration Board (2019-2021). He also was a representative of the University of Urbino within CINECA, GARR, and CRUI (2014-2020).

In his management activity he significantly contributed to digitalization, by originating and supervising among others the project UniDem - Integrated System for the Dematerialization of University Administration Forms and Processes, including the open-source applications UniContr and UniConv that in 2020 were made available for reuse purposes to the Public Administration and integrated

in the professional community Sinallagma of LineaPA. Moreover he directed the design, deployment, and maintenance of Moodle platforms and webconference and e-proctoring tools to support blended learning and e-learning activities as well as distance exams and their integrity.

2. Scientific Curriculum of the associated investigators

1. ROSSI Sabina

Sabina Rossi received her master degree in Mathematics from the University of Padova, Italy, in 1990 and her Ph.D. in Computational Mathematics and Informatics Mathematics from the University of Padova in 1994. She is Associate Professor of Computer Science at the University Ca' Foscari of Venice, Italy, since 2012. Formerly she has been Assistant Professor of Computer Science at the University Ca' Foscari of Venice, Italy, since 2000. Previously, she held a research position at the Universitè Catholique de Louvain-la-Neuve, Belgium. She has been visiting Professor at the Universitè Paris 7, Denis Diderot, France (2007).
She obtained the Italian National Scientific Qualification for the role of Full Professor in Computer Science (ASN 2016-2018, SC: 01/B1 INFORMATICA, SSD: INF/01 INFORMATICA, I Fascia, valid from 07/08/2018 to 07/08/2027.)
She has expertise in foundational models of distributed systems with mobility and concurrency.

Her current research focuses on the development of formal tools for the analysis, verication and performance evaluation of complex systems based on process algebraic techniques. Recently, she has worked on Markovian models for the evaluation of the performance and dependability of computer and communication systems. Specifically, she worked on a new notion of time-reversibility to efficiently compute the stationary probabilities of large Markov models. She has applied her results for the analysis of ad-hoc wireless and sensor networks, systems with fork-join operations, distributed systems with load balancing.
Previously, her research focused on formal models for the specification and verification of security properties in distributed systems, proof techniques for the analysis of cryptographic protocols, formal methods for controlling information release in imperative and concurrent programs, analysis and verification of declarative programs and in particular she contributed to the development of a static analyzer for Prolog. Sabina Rossi was co-director of the groups that developed the following tools:
- CoPs: Checker of Persistent Security: a tool for verifying persistent non-interference properties of CCS processes,
- PicNIc- Pi-calculus Non-Interference checker: a tool for verifying non-interference properties of processes in the Pi-calculs.

Prof. Sabina Rossi has numerous ongoing collaborations with important international research centers: University of Padova, University of Udine, University of Edinburgh, University of Oxford. Se has co-chaired the 11th International Conference on Performance Evaluation Methodologies and Tools (Valuetools 2017) and she is guest associate editor of the Special Issue (IF: 1.613) that will appear in the journal Performance Evaluation (Elsevier). Se has served on the program committees of many international conferences, among which several premier conferences, such as Valuetools, CCNC, EPEW, IFIP Wireless Days, LOPSTR. She gave the tutorial "A Calculus for Power-aware Multicast Communications in Ad Hoc Networks" at the 6th IFIP International Conference on Theoretical Computer Science (TCS'10).

Prof. Sabina Rossi has been principal investigator of the projects:
- "Studio ed implementazione di modelli formali per l'analisi di reti mobili: reti ad hoc e reti di sensori", Fondo per il sostegno dei giovani e per favorire la mobilita degli studenti (MIUR), and
- "Metodi Formali per l'Analisi delle Prestazioni: Reversibilita e Forme Prodotto nelle Catene di Markov", IRIDE - Research incentive, Department of Environmental Sciences, Informatics and Statistics, University Ca' Foscari.

She has participated in several national and international projects: ECOMOBILITY: ECOlogical supporting for traffic Management in cOastal areas By using an InteLlIgenT sYstem (INTERREG Italia-Croazia, 2018-2019), ADAPT - Accessible Data for Accessible Proto-Types in Social Sector (MIUR, SCN_00447, 2015-2017), CINA - Compositionality, Interaction, Negotiation and Autonomicty (MIUR, 2013-2016), "MyThS: Models and Types for Security in Mobile Distributed Systems", (EU Contract IST-2001-32617), just to name a few.

Prof. Sabina Rossi is the (co-)author of over 100 technical papers in refereed international journals and conference proceedings. She received two best paper awards: "A Framework for Throughput and Energy Efficiency in Mobile ad Hoc Networks", IFIP Wireless Days 2011, IEEE Press (2011) and "Fair workload distribution for multi-server systems with pulling strategies", International Conference on Performance Evaluation Methodologies and Tools, Valuetools 2016 (2016).

Prof. Sabina Rossi is member of the board of the doctoral program in Computer Science of Ca' Foscari, she has been member of the Teaching Committee of the BSc and MSc programs in Computer Science at Ca' Foscari, she is member of the ACADIA Research Centre (AdvanCes in Autonomous, DIstributed and pervAsive systems) which brings together researchers in the fields of performance evaluation, program verification and cyber security with the aim of stimulating new collaborations.

According to Scopus (2020-01-05), her h-index is 13 and her papers have been cited 613 times.
According to Google Scholar (2020-01-05), her h-index is 18 and her papers have been cited 1175 times.

2. PIAZZA Carla

Academic Degrees
1. Master degree in Mathematics at the University of Parma with full marks (cum laude) on July 14th, 1997.
The title of the thesis: "Analisi e Definizione di Linguaggi di Set-Constraint". Advisors Prof. Gianfranco Rossi.
2. PhD in Computer Science at the University of Udine on March 15th 2002. The title of PhD thesis: "Computing in Non Standard Set Theories". Supervisor Prof. Alberto Policriti.

Grants
1. During the period December 2001-November 2003 PostDoc position at the Department of Computer Science of the University Ca' Foscari of Venezia. Title of the grant "Computational Models and Semantics". Supervisor Prof. Agostino Cortesi.
2. During the period December 2003-June 2004 European Grant on the project "Models and Types for Security in Mobile Distributed Systems (MyThS)" at the Department of Computer Science of the University Ca' Foscari of Venezia. Supervisor Prof. Michele Bugliesi.
3. During the period July 2004-December 2004 PostDoc position at the Department of Computer Science of the University of Udine.
Title of the grant "Model Checking Techniques in the Analysis of Biological Systems". Supervisor Prof. Alberto Policriti.
4. During the period September 2004-December 2004 grant from
the Area Science Park of Trieste to visit the Bioinformatics group, Courant Institute, New York University. Title of the grant "Formal Verification Techniques for the Analysis of Biological Systems". Supervisor Prof. Bud Mishra.

Employment History
1. January 2005-October 2005. Researcher (Assistant Professor) INF01, University of Udine.
2. November 2005-present. Associate Professor INF01, University of Udine.
3. May 2018. Awarded with the Italian National Scientific Qualification as Full Professor.

Teaching Activity
1. B.S. Courses: Algorithms and Data Structures - B.S. in Multimedia and Web Technologies, B.S. in Computer Science, B.S. in Internet of Things, Big Data & Web (2005--present), Computer Science II - B.S. in Mathematics (2002--2006), Lab. of Algorithms and Data Structures - B.S. in Computer Science (2002--2004).
2. M.S. Courses: Model Checking - M.S. in Computer Science (2005), Algorithms and Complexity -M.S. in Computer Science (2006--2017), Complexity and Information Theory M.S. in Computer Science (2018-present).

Research Interests
Formal Methods.
Model Checking.
Information Flow Security.
Hybrid Systems.
Bioinformatics.

Organization and Participation to Conferences/Workshops
- Speaker in more than 20 international scientific conferences and workshops.
- Member of Program Committees, Organizing Committees, Steering Committees of more than 20 Conferences /Schools/Workshops of international relevance.
- Invited Tutorial. Systems Biology: Models and Logics. Italian Conference on Computational Logic (CILC'08). Perugia, July 2008.
- Invited Talk. Hybrid Automata and Systems Biology. Discrete Models in Systems Biology Workshop. SAMSI North Carolina, December 2008.
- Invited Tutorial. Systems Biology: Models and Logic. International Conference on Logic Programming (ICLP'08). Udine, December 2008.
- Program Co-Chair with Prof. T. Dang of HSB 2013 - International Workshop on Hybrid Systems and Biology. Taormina, September 2013.
- Program Co-Chair with Prof. F. Fages of FMMB 2014 - International Conference on Formal Methods for Macro Biology. Noumea, September 2014.
- Program Co-Chair with Prof. A. Peron of GandALF 2014 - International Symposium on Games, Automata, Logics and Formal Verification. Verona, September 2014.

Activity within PhD schools
- Member of the committee of the PhD school in Computer Science of the University of Udine since 2006.
- Course on Hybrid Automata for the PhD course in Computer Science of the University of Udine in 2012.
- Member of the defence committee of Dr. R. Testylier PhD student at Verimag Grenoble in 2012. - Co-supervisor with Prof. H. Oktem of Dr. N. Gokgoz PhD student at Middle East Technical University of Ankara. Dr. N. Gokgoz obtained her PhD in 2014.
- Co-supervisor with Prof. T. Dang of Dr. T. Dreossi PhD student at University of Udine and University of Grenoble-Alpes. Dr. T. Dreossi obtained his PhD in 2016.

- Co-supervisor with Prof. P. Zuliani of L. Anticoli PhD student at University of Udine. Dr. L. Anticoli obtained her PhD in 2018.

Research Fellowships and Periods Abroad
- Visiting at Institute for Logic, Language and Computation of the University of Amsterdam, The Netherlands. January 2000-July 2000.
- Visiting at Departamento de Sistemas Informaticos y Computacion of the University of Valencia, Spain. April 2001.
- Research Fellow at NYU/Courant Bioinformatics Group of Prof. B. Mishra during the periods: - September-December 2004 - March 2007 - November 2007 – November-December 2008.

Editorial Activity
- Member of the Editorial Board of the journal "Algorithms" (ISSN 1999-4893).
- Editor with Prof. T. Dang of the proceedings of HSB 2013 - Second International Workshop on Hybrid Systems and Biology. EPTCS 125.
- Editor with Prof. A. Peron of the proceedings of GandALF 2014 - Fifth International Symposium on Games, Automata, Logics and Formal Verification. EPTCS 161.
- Editor with Prof. F. Fages of the proceedings of 1st International Conference on Formal Methods in Macro-Biology, FMMB 2014, Lecture Notes in Computer Science, Volume 8738 LNBI, 2014.
- Editor with Proff. O. Maler, A. Halász, and T. Dang of the post-proceedings of the 2nd International Workshop on Hybrid Systems Biology, HSB 2013 and 3rd International Workshop on Hybrid Systems Biology, HSB 2014. Lecture Notes in Computer Science Volume 7699, 2015.
- Guest Editor with Prof. A. Peron of the special issue of Information and Computation containing extended versions of selected papers from GandALF 2014.

Main publications
1 invited chapter; more than 30 papers on international journals; more than 50 international conferences and workshops among which 3 invited; 5 editors of volumes/issues.

Reviewer Activity
AMS Mathematical Reviews; McGraw-Hill; Information and Computation; Theoretical Computer Science; Constraints; Journal of Applied Logic; IEEE Transaction on Automated Control; CL Computer Languages; Automatica; ACM Transactions on Information and System Security; Frontiers of Computer Science; Algorithms for Molecular Biology, Fundamenta Informaticae; many international conferences.

Recent Research Projects
- GNCS INDAM 2020. “Automazione del ragionamento non-monotono su moderne architetture parallele”. Udine unit member.
- GNCS INDAM 2019. "Logic Programming for early de- tection of pancreatic cancer”. Udine unit member.
- GNCS INDAM 2018. "Metodi formali per la verifica e sintesi di sistemi discreti e ibridi”. Udine unit member.
- GNCS INDAM 2017. ”Logica e Automi per il Model- Checking Intervallare”. Udine unit member.
- GNCS INDAM 2016. "Logica, Automi e Giochi per Sis- temi Auto- adattivi". Udine unit member.
- GNCS INDAM 2015. National Coordinator. "Algoritmica per il model checking e la sintesi di sistemi safety-critical".
- PRID 2017. Project Coordinator. "ENCASE: Efforts in the uNderstanding of Complex interActing SystEms".

Technological Transfer
- Collaboration with Acritas s.r.l. for the implementation of software tools for products configuration, management and optimization of photovoltaic systems. The cooperation by Acritas and through the regional project FVG 2008-2009: "Techniques and Algorithms for knowledge representation and manipulation in configuration systems". Some results are reported in "Morphos configuration engine: The core of a commercial configuration system in CLP(FD)", D. Campagna , C. De Rosa , A. Dovier, A. Montanari, C. Piazza, Fundamenta Informaticae, Volume 105, Issue 1-2, 2010, Pages 105-133.
- Collaboration with Tellus S.p.A. for the definition and implementation of time-dependent routing algorithms. Tellus has financed an annual grant "SISTEMA DI PIANIFICAZIONE ADATTIVA PER SOLUZIONI DI MOBILITÀ SOSTENIBILE" in the period 2013-2014. The developed software is in use in Tellus.

Other Software Development
Partecipation in the development of the following tools: Morphos Configuration Engine, SAHA- Tool (A tool for Semi-Algebraic Hybrid Automata analysis), ProPesca (A tool for Gene Profiling Analysis), PicNIc (Pi calculus Non Interference checker), CoPS (Checker of Persistent Security), BANANA (Boundary Ambients Nesting ANAlysis), Fast Bisimulation Algorithm, The {log} Interpreter.

3. Main Principal Investigator's scientific publications (Max. 20)

1. Berardinelli, Luca, Bernardo, Marco, Cortellessa, Vittorio, Di Marco, Antinisca (2019). Multidimensional Context Modeling Applied to Non-Functional Analysis of Software. SOFTWARE AND SYSTEMS MODELING, vol. 18, p. 2137-2176, ISSN: 1619-1366, doi: 10.1007/s10270-017-0645-2 - **Articolo in rivista**
2. Bernardo, Marco, Miculan, Marino (2019). Constructive Logical Characterizations of Bisimilarity for Reactive Probabilistic Systems. THEORETICAL COMPUTER SCIENCE, vol. 764, p. 80-99, ISSN: 0304-3975, doi: 10.1016/j.tcs.2018.12.003 - **Articolo in rivista**
3. Bernardo, Marco (2018). ULTraS at Work: Compositionality Metaresults for Bisimulation and Trace Semantics. THE JOURNAL OF LOGICAL AND ALGEBRAIC METHODS IN PROGRAMMING, vol. 94, p. 150-182, ISSN: 2352-2208, doi: 10.1016/j.jlamp.2017.10.002 - **Articolo in rivista**
4. Bernardo, Marco, Corradini, Flavio, Tesei, Luca (2016). Timed Process Calculi with Deterministic or Stochastic Delays: Commuting between Durational and Durationless Actions. THEORETICAL COMPUTER SCIENCE, vol. 629, p. 2-39, ISSN: 0304-3975, doi: 10.1016/j.tcs.2016.02.022 - **Articolo in rivista**
5. Bernardo, Marco (2015). On the Tradeoff between Compositionality and Exactness in Weak Bisimilarity for Integrated-Time Markovian Process Calculi. THEORETICAL COMPUTER SCIENCE, vol. 563, p. 99-143, ISSN: 0304-3975, doi: 10.1016/j.tcs.2014.10.025 - **Articolo in rivista**
6. Bernardo, Marco, De Nicola, Rocco, Loreti, Michele (2015). Revisiting Bisimilarity and its Modal Logic for Nondeterministic and Probabilistic Processes. ACTA INFORMATICA, vol. 52, p. 61-106, ISSN: 0001-5903, doi: 10.1007/s00236-014-0210-1 - **Articolo in rivista**
7. Bernardo, Marco, De Nicola, Rocco, Loreti, Michele (2014). Relating Strong Behavioral Equivalences for Processes with Nondeterminism and Probabilities. THEORETICAL COMPUTER SCIENCE, vol. 546, p. 63-92, ISSN: 0304-3975, doi: 10.1016/j.tcs.2014.03.001 - **Articolo in rivista**
8. Bernardo, Marco, De Nicola, Rocco, Loreti, Michele (2014). Revisiting Trace and Testing Equivalences for Nondeterministic and Probabilistic Processes. LOGICAL METHODS IN COMPUTER SCIENCE, vol. 10, p. 1-42, ISSN: 1860-5974, doi: 10.2168/LMCS-10(1:16)2014 - **Articolo in rivista**
9. Bernardo, Marco, De Nicola, Rocco, Loreti, Michele (2013). A Uniform Framework for Modeling Nondeterministic, Probabilistic, Stochastic, or Mixed Processes and their Behavioral Equivalences. INFORMATION AND COMPUTATION, vol. 225, p. 29-82, ISSN: 0890-5401, doi: 10.1016/j.ic.2013.02.004 - **Articolo in rivista**
10. Aldini, Alessandro, Bernardo, Marco (2011). Component-Oriented Verification of Noninterference. JOURNAL OF SYSTEMS ARCHITECTURE, vol. 57, p. 282-293, ISSN: 1383-7621, doi: 10.1016/j.sysarc.2010.06.005 - **Articolo in rivista**
11. Bernardo, Marco, Bontà, Edoardo, Aldini, Alessandro (2010). Handling Communications in Process Algebraic Architectural Description Languages: Modeling, Verification, and Implementation. THE JOURNAL OF SYSTEMS AND SOFTWARE, vol. 83, p. 1404-1429, ISSN: 0164-1212, doi: 10.1016/j.jss.2010.02.025 - **Articolo in rivista**
12. Aldini, Alessandro, Bernardo, Marco (2007). A Formal Approach to the Integrated Analysis of Security and QoS. RELIABILITY ENGINEERING & SYSTEM SAFETY, vol. 92, p. 1503-1520, ISSN: 0951-8320, doi: 10.1016/j.ress.2006.10.003 - **Articolo in rivista**
13. Bernardo, Marco (2007). Non-Bisimulation-Based Markovian Behavioral Equivalences. JOURNAL OF LOGIC AND ALGEBRAIC PROGRAMMING, vol. 72, p. 3-49, ISSN: 1567-8326, doi: 10.1016/j.jlap.2007.02.002 - **Articolo in rivista**
14. Aldini, Alessandro, Bernardo, Marco (2005). On the Usability of Process Algebra: An Architectural View. THEORETICAL COMPUTER SCIENCE, vol. 335, p. 281-329, ISSN: 0304-3975, doi: 10.1016/j.tcs.2004.10.043 - **Articolo in rivista**
15. Bernardo, Marco, Bravetti, Mario (2003). Performance Measure Sensitive Congruences for Markovian Process Algebras. THEORETICAL COMPUTER SCIENCE, vol. 290, p. 117-160, ISSN: 0304-3975, doi: 10.1016/S0304-3975(01)00090-1 - **Articolo in rivista**
16. Bernardo, Marco, Ciancarini, Paolo, Donatiello, Lorenzo (2002). Architecting Families of Software Systems with Process Algebras. ACM TRANSACTIONS ON SOFTWARE ENGINEERING AND METHODOLOGY, vol. 11, p. 386-426, ISSN: 1049-331X, doi: 10.1145/606612.606614 - **Articolo in rivista**
17. Bernardo, Marco, Mezzina, Claudio Antares (2020). Towards Bridging Time and Causal Reversibility. In: (a cura di): Gotsman A.;Sokolova A., Proc. of the 40th Int. Conf. on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2020). LECTURE NOTES IN COMPUTER SCIENCE, vol. 12136, p. 22-38, Springer, ISBN: 978-3-030-50085-6, ISSN: 0302-9743, Valletta (Malta), June 2020, doi: 10.1007/978-3-030-50086-3_2 - **Contributo in Atti di convegno**
18. Aldini, Alessandro, Bernardo, Marco (2009). A General Framework for Nondeterministic, Probabilistic, and Stochastic Noninterference. In: (a cura di): Degano P.;Viganò L., Proc. of the 1st Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA/WITS 2009). LECTURE NOTES IN COMPUTER SCIENCE,

vol. 5511, p. 18-33, Springer, ISBN: 9783642034589, ISSN: 0302-9743, York (UK), March 2009, doi: 10.1007/978-3-642-03459-6_2 - **Contributo in Atti di convegno**

19. Aldini, Alessandro, Bernardo, Marco (2009). Weak Behavioral Equivalences for Verifying Secure and Performance-Aware Component-Based Systems. In: (a cura di): De Lemos R.;Fabre J.-C.;Gacek C.;Gadducci F.;ter Beek M.H., Architecting Dependable Systems 6. LECTURE NOTES IN COMPUTER SCIENCE, vol. 5835, p. 228-254, Springer, ISBN: 9783642102479, ISSN: 0302-9743, doi: 10.1007/978-3-642-10248-6_10 - **Contributo in volume (Capitolo o Saggio)**

20. Aldini, Alessandro, Bernardo, Marco, Corradini, Flavio (2010). A Process Algebraic Approach to Software Architecture Design. p. 1-304, Springer, ISBN: 9781848002227, doi: 10.1007/978-1-84800-223-4 - **Monografia o trattato scientifico**

4. Main scientific publications of the associated investigators (Max. 20, for each research unit)

1. **ROSSI Sabina**

1. Marin A., Rossi S., Sottana M. (2020). Dynamic resource allocation in fork-join queues. ACM TRANSACTIONS ON MODELING AND PERFORMANCE EVALUATION OF COMPUTING SYSTEMS, vol. 5, p. 1-28, ISSN: 2376-3639, doi: 10.1145/3372376 - **Articolo in rivista**
2. Bujari A., Marin A., Palazzi C. E., Rossi S. (2019). Smart-RED: A novel congestion control mechanism for high throughput and low queuing delay. WIRELESS COMMUNICATIONS AND MOBILE COMPUTING, vol. 2019, p. 1-10, ISSN: 1530-8669, doi: 10.1155/2019/6941248 - **Articolo in rivista**
3. Giacomo Alzetta, Andrea Marin, PIAZZA, Carla, Sabina Rossi (2018). Lumping-based equivalences in Markovian automata: Algorithms and applications to product-form analyses. INFORMATION AND COMPUTATION, vol. 260, p. 99-125, ISSN: 1090-2651, doi: 10.1016/j.ic.2018.04.002 - **Articolo in rivista**
4. Marin, Andrea, Rossi, Sabina, BURATO, DARIO, Sina, Andrea, Sottana, Matteo (2018). A Product-Form Model for the Performance Evaluation of a Bandwidth Allocation Strategy in WSNs. ACM TRANSACTIONS ON MODELING AND COMPUTER SIMULATION, vol. 28, p. 1-23, ISSN: 1049-3301, doi: 10.1145/3155335 - **Articolo in rivista**
5. MARIN, Andrea, ROSSI, Sabina (2017). Fair workload distribution for multi-server systems with pulling strategies. PERFORMANCE EVALUATION, vol. 113, p. 26-41, ISSN: 0166-5316, doi: 10.1016/j.peva.2017.04.005 - **Articolo in rivista**
6. MARIN, Andrea, ROSSI, Sabina (2017). On the relations between Markov chain lumpability and reversibility. ACTA INFORMATICA, vol. 54, p. 447-485, ISSN: 1432-0525, doi: 10.1007/s00236-016-0266-1 - **Articolo in rivista**
7. MARIN, Andrea, ROSSI, Sabina (2017). Power control in saturated fork-join queueing systems. PERFORMANCE EVALUATION, vol. 116, p. 101-118, ISSN: 0166-5316, doi: 10.1016/j.peva.2017.08.008 - **Articolo in rivista**
8. Bujiari, Armir, MARIN, Andrea, ROSSI, Sabina, Palazzi, Claudio (2016). Analysis of ECN/RED and SAP-LAW with simultaneous TCP and UDP traffic. COMPUTER NETWORKS, vol. 108, p. 160-170, ISSN: 1389-1286, doi: 10.1016/j.comnet.2016.08.016 - **Articolo in rivista**
9. BUGLIESI, Michele, GALLINA, LUCIA, S. Hamadou, MARIN, Andrea, ROSSI, Sabina (2014). Behavioural equivalences and interference metrics for mobile ad-hoc networks. PERFORMANCE EVALUATION, vol. 73, p. 41-72, ISSN: 0166-5316, doi: 10.1016/j.peva.2013.11.003 - **Articolo in rivista**
10. L. Gallina, S. Rossi (2013). A Process Calculus for Energy-Aware Multicast Communications of Mobile Ad-Hoc Networks. WIRELESS COMMUNICATIONS AND MOBILE COMPUTING, vol. 13, p. 296-312, ISSN: 1530-8669, doi: 10.1002/wcm.2207 - **Articolo in rivista**
11. BOSSI A., C. PIAZZA, S. ROSSI (2007). Compositional information flow security for concurrent programs. JOURNAL OF COMPUTER SECURITY, vol. 15, p. 373-416, ISSN: 0926-227X - **Articolo in rivista**
12. CRAFA S, ROSSI S. (2007). Controlling Information Release in the pi-calculus. INFORMATION AND COMPUTATION, vol. 285 , p. 1235-1273, ISSN: 0890-5401, doi: 10.1016/j.ic.2007.01.001 - **Articolo in rivista**
13. FOCARDI R, ROSSI S. (2006). Information Flow Security in Dynamic Contexts. JOURNAL OF COMPUTER SECURITY, vol. 14, p. 65-110, ISSN: 0926-227X - **Articolo in rivista**
14. BOSSI A., D. MACEDONIO, C. PIAZZA, S. ROSSI (2005). Information Flow in Secure Contexts. JOURNAL OF COMPUTER SECURITY, vol. 13, p. 391-422, ISSN: 0926-227X - **Articolo in rivista**
15. BUGLIESI M, ROSSI S. (2005). Non-Interference Proof Techniques for the Analysis of Cryptographic Protocols. JOURNAL OF COMPUTER SECURITY, vol. 13, p. 87-113, ISSN: 0926-227X - **Articolo in rivista**
16. BOSSI A., FOCARDI R., PIAZZA C., ROSSI S. (2004). Verifying Persistent Security Properties.. COMPUTER LANGUAGES, SYSTEMS & STRUCTURES, vol. 30, p. 231-258, ISSN: 1477-8424, doi: 10.1016/j.cl.2004.02.005 - **Articolo in rivista**
17. Ivan Malakhov, Andrea Marin, Sabina Rossi, Daria Smuseva (2020). Fair Work Distribution on Permissioned Blockchains: a Mobile Window Based Approach. In: 2020 IEEE International Conference on Blockchain (Blockchain). vol. 1, p. 436-441, IEEE Computer Society, ISBN: 978-0-7381-0495-9, doi: 10.1109/Blockchain50366.2020.00063 - **Contributo in Atti di convegno**
18. Hillston J., Piazza C., Marin A., Rossi S. (2019). Delimited persistent stochastic non-interference. In: ACM International Conference Proceeding Series. p. 135-142, 1515 BROADWAY, NEW YORK, NY 10036-9998 USA:Association for Computing Machinery, ISBN: 9781450365963, Universitat de les Illes Balears, esp, 2019, doi: 10.1145/3306309.3306329 - **Contributo in Atti di convegno**
19. Marin A., Piazza C., Rossi S. (2019). A process algebra for (delimited) persistent stochastic non-interference. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). LECTURE NOTES IN ARTIFICIAL INTELLIGENCE, vol. 11785, p. 222-238, Springer Verlag, ISBN: 9783030302801, ISSN: 0302-9743, gbr, 2019, doi: 10.1007/978-3-030-30281-8_13 - **Contributo in Atti di convegno**

20. Hillston, Jane, Marin, Andrea, Piazza, Carla, Rossi, Sabina (2018). Information Flow Security for Stochastic Processes. In: (a cura di): Rena Bakhshi Paolo Ballarini Benoît Barbot Hind Castel-Taleb Anne Remke, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). vol. 11178, p. 142-156, Springer Verlag, ISBN: 9783030022266, fra, 2018, doi: 10.1007/978-3-030-02227-3_10 - **Contributo in Atti di convegno**

2. **PIAZZA Carla**

1. Alzetta, Giacomo, Marin, Andrea, Piazza, Carla, Rossi, Sabina (2018). Lumping-based equivalences in Markovian automata: Algorithms and applications to product-form analyses. INFORMATION AND COMPUTATION, vol. 260, p. 99-125, ISSN: 0890-5401, doi: 10.1016/j.ic.2018.04.002 - **Articolo in rivista**
2. DREOSSI, Tommaso, Dang, Thao, PIAZZA, Carla (2017). Reachability computation for polynomial dynamical systems. FORMAL METHODS IN SYSTEM DESIGN, vol. 50, p. 1-38, ISSN: 0925-9856, doi: 10.1007/s10703-016-0266-3 - **Articolo in rivista**
3. Casagrande, Alberto, PIAZZA, Carla (2015). Unwinding biological systems. THEORETICAL COMPUTER SCIENCE, vol. 587, p. 26-48, ISSN: 0304-3975, doi: 10.1016/j.tcs.2015.02.045 - **Articolo in rivista**
4. Gentilini, R., PIAZZA, Carla, POLICRITI, Alberto (2015). Rank and simulation: the well-founded case. JOURNAL OF LOGIC AND COMPUTATION, vol. 25, p. 1331-1349, ISSN: 0955-792X, doi: 10.1093/logcom/ext066 - **Articolo in rivista**
5. Casagrande, A., DREOSSI, Tommaso, Fabriková, J., PIAZZA, Carla (2014). -Semantics computations on biological systems. INFORMATION AND COMPUTATION, vol. 236, p. 35-51, ISSN: 0890-5401, doi: 10.1016/j.ic.2014.01.011 - **Articolo in rivista**
6. FRANCESCHET, Massimo, Gubiani, D., MONTANARI, Angelo, PIAZZA, Carla (2013). A graph-theoretic approach to map conceptual designs to XML schemas. ACM TRANSACTIONS ON DATABASE SYSTEMS, vol. 38, ISSN: 0362-5915, doi: 10.1145/2445583.2445589 - **Articolo in rivista**
7. CASAGRANDE, Alberto, PIAZZA, Carla, POLICRITI, Alberto (2009). Discrete Semantics for Hybrid Automata. DISCRETE EVENT DYNAMIC SYSTEMS, vol. 19, p. 471-493, ISSN: 0924-6703, doi: 10.1007/s10626-009-0082-7 - **Articolo in rivista**
8. CASAGRANDE, ALBERTO, PIAZZA, Carla, POLICRITI, Alberto, MISHRA, BUD (2008). Inclusion dynamics hybrid automata. INFORMATION AND COMPUTATION, vol. 206, p. 1394-1424, ISSN: 0890-5401, doi: 10.1016/j.ic.2008.09.001 - **Articolo in rivista**
9. GENTILINI, R., PIAZZA, Carla, POLICRITI, Alberto (2008). Symbolic Graphs: Linear Solutions to Connectivity Related Problems. ALGORITHMICA, vol. 50, p. 120-158, ISSN: 0178-4617, doi: 10.1007/s00453-007-9079-5 - **Articolo in rivista**
10. BOSSI, A., PIAZZA, Carla, ROSSI, S. (2007). Compositional information flow security for concurrent programs. JOURNAL OF COMPUTER SECURITY, vol. 15, p. 373-416, ISSN: 0926-227X, doi: 10.3233/JCS-2007-15303 - **Articolo in rivista**
11. BOSSI A, MACEDONIO D, PIAZZA, Carla, ROSSI S. (2005). Information flow in secure contexts. JOURNAL OF COMPUTER SECURITY, vol. 13, p. 391-422, ISSN: 0926-227X, doi: 10.3233/JCS-2005-13303 - **Articolo in rivista**
12. BOSSI A., FOCARDI R., PIAZZA, Carla, ROSSI S. (2004). Verifying Persistent Security Properties. COMPUTER LANGUAGES, SYSTEMS & STRUCTURES, vol. 30, p. 231-258, ISSN: 1477-8424, doi: 10.1016/j.cl.2004.02.005 - **Articolo in rivista**
13. DOVIER, Agostino, PIAZZA, Carla, POLICRITI, Alberto (2004). An Efficient Algorithm for Computing Bisimulation Equivalence. THEORETICAL COMPUTER SCIENCE, vol. 311, p. 221-256, ISSN: 0304-3975, doi: 10.1016/S0304-3975(03)00361-X - **Articolo in rivista**
14. DOVIER, Agostino, PIAZZA, Carla (2003). The Subgraph Bisimulation Problem. IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, vol. 15, p. 1055-1056, ISSN: 1041-4347, doi: 10.1109/TKDE.2003.1209024 - **Articolo in rivista**
15. Hillston, Jane, Piazza, Carla, Marin, Andrea, Rossi, Sabina (2019). Delimited persistent stochastic non-interference. In: ACM International Conference Proceeding Series. p. 135-142, Association for computing machinery, ISBN: 9781450365963, Universitat de les Illes Balears, esp, 2019, doi: 10.1145/3306309.3306329 - **Contributo in Atti di convegno**
16. Marin A., Piazza C., Rossi S. (2019). A process algebra for (delimited) persistent stochastic non-interference. In: 16th International Conference on Quantitative Evaluation of Systems, QEST 2019. LECTURE NOTES IN COMPUTER SCIENCE, vol. 11785, p. 222-238, Springer Verlag, ISBN: 978-3-030-30280-1, ISSN: 0302-9743, gbr, 2019, doi: 10.1007/978-3-030-30281-8_13 - **Contributo in Atti di convegno**
17. Marin A., Piazza C., Rossi S. (2019). Proportional Lumpability. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). vol. 11750, p. 265-281, Springer, ISBN: 978-3-030-29661-2, nld, 2019, doi: 10.1007/978-3-030-29662-9_16 - **Contributo in Atti di convegno**
18. Hillston, Jane, Marin, Andrea, Piazza, Carla, Rossi, Sabina (2018). Information Flow Security for Stochastic Processes. In: 15th European Performance Engineering Workshop. vol. 11178, p. 142-156, Paris; France, 29-30 ottobre 2018, doi: 10.1007/978-3-030-02227-3_10 - **Contributo in Atti di convegno**
19. Hillston, Jane, Piazza, Carla, Rossi, Sabina (2018). Persistent stochastic non-interference. In: Combined 25th International Workshop on Expressiveness in Concurrency and 15th Workshop on Structural Operational Semantics, EXPRESS/SOS 2018. ELECTRONIC PROCEEDINGS IN THEORETICAL COMPUTER SCIENCE, vol. 276, p. 53-68, ISSN: 2075-2180, Beijing; China, 3 settembre 2018, doi: 10.4204/EPTCS.276.6 - **Contributo in Atti di convegno**
20. Matteo Sottana, Carla Piazza, Andrea Albarelli (2017). Efficient Computation of Renaming Functions for -reversibility Discrete and Continuous Time Markov Chains. In: VALUETOOLS 2017. Proceedings of the 11th EAI International Conference on Performance Evaluation Methodologies and Tools. p. 52-59, ACM, Venice, December 05 - 07, 2017 - **Contributo in Atti di convegno**

5. Main staff involved (max 10 professors/researchers for each research unit, in addition to the PI or associated investigator), highlighting the time commitment expected

List of the Research Units

Unit 1 - BERNARDO Marco

Personnel of the research unit

nº	Surname Name	Qualification	University/ Research Institution	e-mail address	Months/person expected
1.	BERNARDO Marco	Professore Ordinario (L. 240/10)	Università degli Studi di Urbino Carlo Bo	marco.bernardo@uniurb.it	9,0
2.	CARLETTI Margherita	Ricercatore confermato	Università degli Studi di Urbino Carlo Bo	margherita.carletti@uniurb.it	6,0
3.	MEZZINA Claudio Antares	Ricercatore a t.d. - t.pieno (art. 24 c.3-b L. 240/10)	Università degli Studi di Urbino Carlo Bo	claudio.mezzina@uniurb.it	6,0

Unit 2 - ROSSI Sabina

Personnel of the research unit

nº	Surname Name	Qualification	University/ Research Institution	e-mail address	Months/person expected
1.	ROSSI Sabina	Professore Associato (L. 240/10)	Università "Ca' Foscari" VENEZIA	srossi@dsi.unive.it	7,0
2.	BALSAMO Maria Simonetta	Professore Ordinario	Università "Ca' Foscari" VENEZIA	balsamo@dsi.unive.it	4,0

Unit 3 - PIAZZA Carla

Personnel of the research unit

nº	Surname Name	Qualification	University/ Research Institution	e-mail address	Months/person expected
1.	PIAZZA Carla	Professore Associato confermato	Università degli Studi di UDINE	carla.piazza@uniud.it	11,0
2.	FABRIS Francesco	Professore Associato confermato	Università degli Studi di TRIESTE	ffabris@units.it	2,0

6. Information on the new contracts for personnel to be specifically recruited

nº	Associated or principal investigator	Number of expected RTD contracts	Number of research grants expected	Number of PhD scholarships expected	Overall expected time commitment (months)
1.	BERNARDO Marco	0	1	0	24
2.	ROSSI Sabina	0	1	0	24
3.	PIAZZA Carla	0	1	0	24
	Total	**0**	**3**	**0**	**72**

"The data contained in the application for funding are processed exclusively for carrying out the institutional functions of MUR. The CINECA, Department of Services for MUR, is in charge of the maintenance of these data. The consultation is also reserved to universities and research institutions (each for its respective competence), MUR - Directorate General for coordination and development of research and its results - Office III, CNGR, CdS, and the reviewers in charge of the peer review. MUR also has the right to the dissemination of the main economic and scientific data related to the funded projects".

Date 26/01/2021 ore 13:02