EQIP - Engineering for Quantum Information Processors

- **Project lead: Anthony Leverrier** anthony.leverrier@inria.fr

  Project lead's team and center: COSMIQ, Paris

- **Internal partners (EP/CRI)**
  - CAGE (Paris): Mario Sigalotti mario.sigalotti@inria.fr
  - CASCADE (Paris): Phong Nguyen phong.nguyen@ens.fr
  - COSMIQ (Paris): Anthony Leverrier anthony.leverrier@inria.fr
  - DEDUCTEAM (Saclay): Pablo Arrighi pablo.arrighi@univ-amu.fr
  - GRACE (Saclay): Alain Couvreur alain.couvreur@inria.fr
  - HiePACS (Bordeaux): Emmanuel Agullo emmanuel.agullo@inria.fr
  - MATHERIALS (Paris): Claude Le Bris claude.le-bris@enpc.fr
  - MOCQUA (Nancy): Simon Perdrix simon.perdrix@loria.fr
  - PACAP (Rennes): Caroline Collange caroline.collange@inria.fr
  - PARSYS (Saclay): Marc Baboulin marc.baboulin@universite-paris-saclay.fr
  - QUANTIC (Paris): Mazyar Mirrahimi mazyar.mirrahimi@inria.fr
  - STORM (Bordeaux): Denis Barthou denis.barthou@inria.fr
- **External partner**
  - Atos Quantum: Cyril Allouche cyril.allouche@atos.net

Three additional teams, CAMBIUM (Paris, François Pottier francois.pottier@inria.fr), McTAO (Sophia, Jean-Baptiste Pomet jean-baptiste.pomet@inria.fr) and TONUS (Nancy, Philippe Helluy philippe.helluy@unistra.fr) are also interested in the topic but would prefer to act as observers for the time being.

Note: four new teams have integrated the consortium since the original letter of intent. These are two HPC teams in Bordeaux, namely HiePACS and STORM, as well as PARSYS in Saclay and the industrial partner Atos Quantum.

Summary Building a functional quantum computer is one of the grand scientific challenges of the 21st century. This formidable task is the object of **Quantum Engineering**, a new and very active field of research at the interface between physics, computer science and mathematics. The goal of the **EQIP** challenge is to bring together all the competences already present in the institute, and to turn Inria into a major international actor in quantum engineering, including both the software and hardware aspects of quantum computing.

Motivation

While the technological development that has led us from the abacus to today's supercomputers or even to the latest achievements of machine learning are quite spectacular, one should not forget that they all fit the very same model of computation, formalized by Turing in the 1930s, and therefore fall under the umbrella of classical computing. Quantum physics has played a major role in this story through the 1^{st} *quantum revolution* which gave birth to the transistor, the laser and the micro-processor. Rather surprisingly, the impact of quantum physics on the theory of computation is very likely still in its infancy. There is little doubt that an unprecedented shift will occur in the decades to come and that an entirely new form of computing will be dominant in 50 years (and probably much sooner). This is the object of the 2^{nd} *quantum revolution* which will harness the quantum properties of matter and light to process data much more efficiently than is possible by purely classical means. The scope of applications remains hard to delineate at this point but covers a large spectrum of human activities: simulation of quantum systems will be crucial to develop new medicine, help fighting climate change by developing better materials to store or transport energy, reducing CO2 emissions by developing efficient processes to capture CO2; quantum computing will also be instrumental to solve optimization problems intractable today. At the same time, quantum technologies will dramatically impact cryptography and requires to implement important changes right now.

If the first glimpse of this second quantum revolution can be traced back to visionaries like Feynman or Deutsch in the early 80s, the fields of quantum computation and quantum simulation really took off in the last decade or so. The long-term objective of this line of work is to build a large universal quantum computer and the main scientific challenges today are to identify potential approaches for scaling up the small quantum processors consisting of a few tens of qubits already available, to anticipate how to program these new machines, and to understand what new capabilities will become accessible once quantum computing becomes available.

Answering these questions requires a wide set of expertises ranging from quantum physics to computer science and mathematics. While these expertises are present at Inria, they tend to be spread over many different project-teams, and in most of these teams, it is usually the case that only one or two researchers work on topics close to quantum computing. This state of affairs is easily explained: given the risky aspect of quantum computing, it is only logical that at first only individual researchers start investigating these questions out of personal interest. Creating entire teams working on such topics requires several researchers to take the same decision, and this can be a long process.

In the present situation, the best strategy for Inria is certainly to foster collaboration between the many teams that work on topics close to quantum computing. This will create a propice environment where individual researchers will get access to the knowledge of their colleagues from other teams. It will also them allow to tackle research problems at the interface of different fields, and to later apply together to French or European calls for projects, something essentially impossible in the current configuration.

Expertise & team boundaries. The EQIP challenge requires expertise in (1) superconducting qubits, (2) simulation of quantum systems, (3) numerical methods, (4) control theory, (5) programming languages and formal methods, (6) compilation, (7) quantum error correction, (8) quantum emulation, (9) cryptography and cryptanalysis, (10) quantum algorithms, (11) high-performance computing.

CAGE has expertise in 2, 4; CAMBIUM, 5; CASCADE, 9; COSMIQ, 7, 9, 10; DEDUCTEAM, 5; GRACE, 7; HiePACS, 11; MATHERIALS, 3; MOCQUA, 5, 10; PACAP, 6; PARSYS, 8, 11; QUANTIC, 1, 2, 4, 7; STORM, 11; and Atos Quantum, 6, 8, 10.

Originality. The large spectrum of expertise gathered in the EQIP consortium might well be unique in the world. Most academic or industrial labs typically focus on a limited number of goals, either on hardware or software solutions. The teams involved in the challenge cover the entire engineering chain starting from hardware aspects such as building new qubits, the whole software stack, to applications.

Scientific synergy. Because the field of quantum technologies is so young, it is rarely part of universities curriculum. This means that most researchers working in this field usually only master a couple of the 11 topics mentioned above, and that most Inria researchers working in the teams involved in the consortium are not at all familiar with quantum technologies or quantum computing. The EQIP challenge will allow them to get acquainted to many new topics in this fast-moving field. In addition, it will offer many opportunities for solving new and relevant problems that often lie at the interface between different disciplines.

Context

International context. Research on quantum computing was almost exclusively performed in academic labs until about 5 years ago, with steady but rather slowly-paced progress in terms of number of controlled qubits for instance. The situation has radically changed in the past few years with IBM, Google, Microsoft, Alibaba and very recently Amazon all starting to invest massively in the field. Together with the ever-growing number of startups appearing notably in North America (and now also in Europe), they are in part responsible for a significant brain drain from academia to the private sector. Several national programs exceeding a billion dollars (sometimes by far) have also been launched around the world, most notably in China and in the United states. Access to quantum computing (and also quantum communication) is perceived as a geostrategic resource and the most powerful countries (or companies) are reluctant to let their competitors build a competitive advantage in this field.

European context. The European Commission launched a 10-year, 1-billion-Euro flagship program on Quantum Technologies in 2017. It is articulated around 4 main pillars: quantum computing, quantum communication, quantum simulation and sensing. Funding for communication (i.e. quantum cryptography) and quantum computing should

continue in the program Horizon Europe, through EuroQCI (quantum communication infrastructure) and EuroHPC, respectively. In particular, a first call for integrating quantum processors with High-Performance Computing (HPC) just appeared this April.

French context. The parliamentary mission led by Paula Forteza delivered In January 2020 a report describing the situation relative to quantum technologies in France and made a series of recommendations. Developing the technologies to build a large-scale quantum computer is now a national priority and a vast program with probably around 1 billion Euro will be launched with this objective in mind. A large part of this program will be devoted to improve hardware approaches to create the qubits needed for a quantum computer, and to develop the software aspects of quantum computing. The main coordinating structures for quantum technologies at the national level are the GdR IQFA and the "groupe de travail informatique quantique" from GdR IM. In the region Ile-de-France, a 4-year 10-million-Euro program (DIM SIRTEQ) was launched in 2017 and is structured around the same pillars as the quantum flagship.

The targeted challenge & expected impact

The EQIP challenge has two main ambitions. The first goal is to **structure the research in quantum computing at Inria**. Right now, this research is spread over a dozen project-teams that barely ever interact. This is all the more wasteful as most of the involved researchers are international leaders in their own field. Creating synergies between them is possible and many topics of collaborations are already outlined below. There is little doubt that new topics will emerge in the coming years. The second ambition of this challenge is **to make Inria a major international actor in quantum engineering**, including both the software and hardware aspects of quantum computing. Right now, the industrial leaders (Google, IBM) are focussing on specific technologies and architectures (e.g., transmon and surface code) and are starting to reach some limitations of these choices. This may lead to a new generation of solutions such as cat qubits or quantum LDPC codes for which Inria is a pioneer. As already mentioned, the talents and expertise are already there (although new hirings could help a great deal), but Inria is not yet perceived as a major player in the field, in part because the different teams do not interact much and tend to publish in different communities.

Given the expertise already present at Inria, we propose the following themes for this challenge: (1) building a quantum processor, (2) developing the software stack needed to operate a large-scale quantum computer, (3) developing quantum solutions to overcome classical computers.

The first question is concerned with engineering problems such as finding the right physical systems to encode quantum information and figuring out how to simulate such systems and how to control them. This will concern mostly the project-teams CAGE, COSMIQ, MATHERIALS and QUANTIC.

The second question has more of a computer-science flavor to it, and addresses the problem of how to efficiently perform computations once many qubits are available. In

particular, we will explore a number of themes ranging from high-level problems such as programming languages and compilation to lower-level problems related to error correction or emulation of quantum systems. The relevant project-teams from Inria are COSMIQ, DEDUCTEAM, GRACE, MOCQUA, PACAP and PARSYS. These will be completed by an industrial partner, Atos Quantum. And other teams not at all involved with quantum computing for the moment have expressed an interest in following the advances concerning these software aspects, namely CAMBIUM, HiePACS and STORM.

The third question deals with the algorithmic aspects of quantum computing. A field where Inria is world-renowned is cryptography and it only makes sense that Inria should also be a world-leader of quantum cryptanalysis: how do quantum computers affect the security of cryptosystems thought to be quantum-resistant? Another topic of interest concerns the power of the near intermediate-scale quantum (NISQ) machines that will become available in the coming years. These questions will be explored by CASCADE, COSMIQ, MOCQUA and QUANTIC. Finally, we are expecting to see a convergence between HPC and quantum technologies in the coming years, and the relevant challenges will be studied in collaboration with HiePACS and STORM.

Scientific impact. A concrete result of the challenge will be to foster collaborations between the different Inria teams, and this should in turn allow them to address scientific questions that may have been out of reach otherwise. Among those, we can mention an in-depth study of the cat-qubit approach to quantum computing, from hardware issues to software questions related to fault tolerance, or the development of a full software stack for quantum computing. Another more prospective question that might uniquely addressed in the challenge is that of the convergence between HPC and quantum computing.

Industrial impact. One of the priorities of the national plan for quantum computing will be to build a full ecosystem around quantum technologies. In particular, it will be crucial to develop partnerships between academia and the industrial world. The presence of an industrial partner, Atos Quantum, in the consortium will be helpful to expose Inria researchers to concrete problems that might interest companies. Some members of the consortium are already working with industrial partners such as EDF or startups like Alice&Bob or QuanFi. The EQIP challenge will likely increase the number of such collaborations and might lead to the creation of new startups.

Scientific approach (a sketch) & organization

For most of the topics developed below, the mentioned teams are among the leaders in their respective communities and the suggested collaborations would allow them to tackle new problems that go significantly beyond what each team would potentially address individually.

The EQIP challenge is built around 3 workpackages:

- **WP1: Building a quantum processor.** This first axis deals with questions at the interface between physics and applied mathematics and its goal is to design and understand systems that can process quantum information.
- **WP2: Operating quantum computers.** The second axis is more long-term and deals with machines consisting of thousands or more qubits. Assuming that we are able to control such large systems, how should one encode quantum information so as to process it efficiently, how should one program such machines?
- **WP3: Overtaking classical computers.** The third axis is concerned with the possibilities offered by quantum processors. What algorithms can be run, notably in the context of cryptanalysis? What kind of applications will be possible with the small quantum processors that will become available in the coming years? How to integrate HPC and quantum computing?

WP1: Building a quantum processor (QUANTIC, CAGE, COSMIQ, MATHERIALS)

- **Goal:** to design and build various components of a hardware-efficient and fault-tolerant quantum processor based on superconducting circuits.
- **Starting point:** QUANTIC and some collaborators pursue a new approach to encode and manipulate a quantum bit of information. This approach, known as cat-qubits, consists of encoding information in Schrödinger cat states of microwave radiation in a superconducting resonator and promises a strong reduction of hardware requirements to implement a fault-tolerant quantum processor.
- **Tasks:** WP1 addresses the complete chain of design, numerical simulations, control and optimization, and experimental realization of the quantum superconducting circuits. It is divided into three tasks:
  - T1.A – Efficient numerical simulation of open quantum systems: MATHERIALS, QUANTIC
  - T1.B – Optimized adiabatic bias-preserving gates for cat-qubits: CAGE, MATHERIALS, QUANTIC
  - T1.C – Optimized error correcting codes for biased noise cat-qubits: COSMIQ, QUANTIC
- **Detailed description:** Many academic and industrial actors around the world have been working on the implementation of long-lived quantum bits with the capacity of performing high-fidelity logical gates. Superconducting circuits (exploited by companies such as Google and IBM among others) represent one of the most advanced physical platforms to realize such quantum bits [1]. On this platform single-qubit and two-qubit logical gates have been demonstrated with fidelities above 99%. The next critical step towards fault-tolerant quantum computation requires the implementation of quantum error correcting codes. The most popular approach corresponds to the so-called toric or surface codes [2], which benefit from a reasonable fault-tolerance threshold of order of half a percent (i.e., each operation at the level of the physical qubits should admit a fidelity above 99.5%). However, this approach comes at the expense of a large hardware overhead (many 100s or 1000s of physical qubits per logical qubit).

  Over the past years, QUANTIC, together with collaborators at Yale University, have developed an alternative approach consisting in encoding the information in the infinite dimensional Hilbert space of a harmonic oscillator (a superconducting resonator) [3, 4, 5]. A nonlinear driven dissipative process confines the information in a two-dimensional manifold [6]. This stabilized qubit (called cat-qubit) benefits from a biased noise where one component of noise (bit-flips) is exponentially suppressed with the amount of energy pumped in the circuit. The recent experiments by QUANTIC have demonstrated a suppression of such bit-flip errors by a factor of 300 and we expect even higher suppressions in the new generations of the experiment [7].

Furthermore, such a cat-qubit also benefits from an extensive set of logical gates which preserve this noise suppression. A preliminary theoretical proposal suggested that this could imply a drastic reduction of hardware requirements for fault-tolerant quantum computation [8]. The main goal of this WP is to push these preliminary ideas towards experimental demonstrations. In this WP, we will also exploit other continuous-variable encodings such as the so-called Gottesman-Kitaev-Preskill (GKP) codes [9, 10] where information is encoded in the grid states of the harmonic oscillator and where both error components are suppressed symmetrically.

The first requirement for a thorough study of these ideas is to develop efficient and precise numerical schemes to simulate the underlying open quantum systems. This is the goal of Task T1.A. While the underlying system is described by a linear master equation, it is defined on a very large Hilbert space (a truncated infinite dimensional Hilbert space), and demonstrating high-fidelity logical gates on large cat-qubits or GKP codes requires a high number of basis states in this truncation. Furthermore, whenever dealing with multi-qubit gates (typically controlled NOT gate or Toffoli gate), we need to work with the tensor product of these spaces with a rapidly exploding dimension. This problem is therefore a mathematical problem, at the intersection of PDE theory and the design of numerical discretization methods, on the reduction of a model. As we can only reduce a system that we understand well (for example because we understood the right "coordinate system" to simulate it), understanding the physics of the problem is central. In short, we need to develop numerical schemes that are strongly inspired by the physics of the system. This will be performed through a collaboration between MATHERIALS and QUANTIC and follows up some previous collaborative results [11, 12].

The goal of Task T1.B is to develop and optimize bias-preserving gates on cat-qubits. By slowly varying the parameters of the driven dissipative mechanism, one can perform various logical gates on qubits where bit-flips remain exponentially suppressed. While the adiabaticity is required for bit-flip suppression, the long duration of these gates expose the cat-qubits to a high probability of phase-flip errors. In T1.B, we propose to exploit the shortcuts to the adiabaticity [13], where by adding some engineered Hamiltonian or dissipation, we can accelerate the quantum operation and therefore improve the overall performance. As an extension, we will also explore the possibility of developing new adiabatic gates on autonomously stabilized GKP codes. This task will be the subject of a collaboration between CAGE and QUANTIC and will benefit from the expertise of MATHERIALS on the numerical side.

Finally, Task T1.C will explore new error correcting codes to suppress the phase-flip errors. Indeed, while a simple repetition code built of a 1D array of cat-qubits can handle such errors, this encoding suffers from two important drawbacks: (1) The decoding process is a non-local mechanism (i.e., requires a global knowledge of all error syndrome measurements before taking any decision on the error correcting action). This strongly limits our capability of engineering autonomous error correction mechanisms where errors are handled directly in hardware and by another controlling quantum system. (2) Some fully-protected logical gates are not transversal and

require a strong connectivity between the qubits. This is an important drawback from the architecture point of view and requires extra experimental developments. In T1.C, we propose to explore alternatives among more advanced codes for such biased noise qubits. This task will involve a collaboration between COSMIQ and QUANTIC.

- **Interaction with other WP:** The noise models will be studied in T2.D on emulation and will be helpful to better understand what cost models should be chosen in the context of cryptanalysis (T3.A). Algorithms exploiting cat-qubits will be investigated in T3.B.
- **External funding/participants:** T1.A will also benefit from ERC Q-Feedback (P. Rouchon, QUANTIC). Also, all experimental efforts related to WP1 will be supported by ERC ECLIPSE (Z. Leghtas, QUANTIC).

WP2: Operating quantum computers (MOCQUA, Atos Quantum, COSMIQ, DEDUCTEAM, GRACE, PACAP, PARSYS). The teams CAMBIUM, HiePACS and STORM expressed interest in following the progress of this WP.

- **Goal:** to develop the tools to program and use large quantum processors.
- **Starting point:** in-depth knowledge of classical programming languages, of quantum error correction, ZX-calculus, emulation of quantum computers.
- **Tasks:**
  - T2.A – Quantum programming language and formal methods: DEDUCTEAM, MOCQUA (+ CAMBIUM)
  - T2.B – Compilation, Optimisation: PACAP, MOCQUA, DEDUCTEAM, PARSYS, Atos Quantum
  - T2.C – Quantum error correcting codes: COSMIQ, GRACE
  - T2.D – Quantum emulation: Atos Quantum, DEDUCTEAM, MOCQUA, PARSYS (+ HiePACS, STORM)
- **Detailed description:**

  Quantum computing is entering the new area of NISQ (Noisy Intermediate-Scale Quantum) devices. Powered by progresses in quantum technologies, these developments point out the necessity of filling the gap between the abstract algorithms and the quantum devices, and to develop the ecosystem for actually using the quantum computer. For instance, major companies like Google or IBM and startups like CQC or Rigetti are working on the development of compilation stacks. Inria teams did not wait for the recent development of NISQ to investigate these questions and already have a leading expertise in these fields: in quantum programming languages [14, 15, 16], error correcting codes [17, 18, 19], circuit optimisation [20, 21, 22, 23], formal methods [24, 25] and models of quantum computing [26].

  This WP intends to gather and further develop this expertise to fill the gap between the high-level abstract quantum algorithms and the quantum machines. Filling this gap, which can be seen as a full compilation stack, consists in developing the theory and the necessary tools to make the quantum computer operable, and also to have a better understanding of the power and the limits of the quantum computer.

  First, quantum programming languages are necessary for programming the quantum computer, taking into account its specificities (like no-cloning) and allowing the description and the development of new quantum algorithms. This is the main goal of Task T2.A. One of the most challenging aspects of working on quantum programming languages is discovering suitable mathematical models that can be exploited to study its program behavior. Quantum programming languages are also necessary to describe quantum programs in practice and to develop libraries of quantum algorithms. Our aim is to reason on quantum computing for proving correctness and

estimating the resources used by a given program. This task will involve both DEDUCTEAM and MOCQUA and also benefit from the expertise of CAMBIUM on classical programming languages.

The objective of Task T2.B is to transform quantum programs into basic instructions implementable on quantum architectures, with the necessary optimisations needed to minimise the resources. Indeed, since the quantum machines available in the near future will have a limited memory and coherent time, optimizing the number of quantum bits and instructions is crucial. Our aim is to provide efficient synthesis and optimisation tools for quantum circuits. In particular, we will explore the possibilities offered in this context by the ZX-calculus, a powerful graphical formalism generalizing quantum circuits and equipped with a complete equational theory allowing for the transformation of quantum codes. One of the main challenges here is to take into account the constraints imposed by the architecture, for instance which operations are available on which qubits of the memory. This task will be performed through a collaboration between DEDUCTEAM, MOCQUA, PACAP and PARSYS.

The aim of near-term machines is to perform useful tasks with a small number of noisy qubits. Longer-term machines are expected to provide exponential speedups for important problems but will require large quantum computers with close-to-ideal logical qubits. Building these large-scale quantum computers will require to implement quantum error correcting techniques and fault-tolerant quantum computing. Task T2.C aims at developing better quantum low-density parity-check (LDPC) codes. While LDPC codes are ubiquitous in the classical context, they remain poorly understood in the quantum case, despite being the best candidate to build large quantum computers. In particular, how good such codes can be, how to decode them efficiently? This task will involve COSMIQ and GRACE.

HPC is closely related to the development of quantum computing, first because quantum computation on a bounded memory can be emulated on a classical computer, and also because most of the quantum algorithms are actually hybrid algorithms. The goal of Task 2.D is to provide the best implementation of a quantum computation (or hybrid classical-quantum computation) on a necessary hybrid computer: how the different parts are intertwined, which quantum parts can be emulated? This task will be performed through a collaboration between Atos Quantum, DEDUCTEAM, PARSYS. The project-teams HiePACS and STORM are also interested by progress on these questions.

- **Interaction with other WP:** Task T2.C is linked to WP1 but considers the problem at a larger scale: aiming to protect many qubits instead of a few.
- **External funding/participants:** This WP is linked to the projects BPI-Quantex and ANR-SoftQPro involving Atos Quantum, DEDUCTEAM, MOCQUA and PARSYS. Collaborations are also currently in progress between DEDUCTEAM and CEA-LIST on the verification of quantum programs and between PACAP and CEA-LIST on the compilation of classical computers with quantum accelerators.

WP3: Overtaking classical computers (COSMIQ, CASCADE, HiePACS, MOCQUA, PARSYS, QUANTIC, STORM)

- **Goal:** exploiting the capabilities of quantum machines to go beyond classical computing.
- **Starting point:** in-depth knowledge of classical cryptanalysis and general purpose quantum algorithms; development of ⋆PU.
- **Tasks:**
  - T3.A – Quantum cryptanalysis: CASCADE, COSMIQ
  - T3.B – NISQ algorithms: COSMIQ, MOCQUA, QUANTIC
  - T3.C – Integration with HPC: HiePACS, PARSYS, STORM
- **Detailed description:**

  The third axis is concerned with the possibilities offered by quantum processors with the goal of overcoming classical computers. A first application which is particularly relevant at Inria is quantum cryptanalysis. Since the discovery of Shor's algorithm, it is known that most of public-key cryptography would be broken by a quantum computer. While the cryptography community took its time to react to this threat, speculating that quantum computers would never be built, this is not the case anymore and a large community with many experts at Inria are working right now to propose new cryptosystems that would remain secure against a quantum adversary. Another, shorter-term, objective for quantum computing is to demonstrate useful algorithms on quantum machines. Such quantum machines might not be large enough to perform Shor's algorithm, notably because they will not possess any error correction mechanism, but could be competitive to solve some relevant optimization problems. Finally, we anticipate the question of the integration of the first quantum accelerators to HPC.

  The first task (T3.A) is devoted to quantum cryptanalysis. To deal with the quantum threat, postquantum cryptosystems have been devised in the past few years and are currently studied in the context of a NIST competition. While most researchers focus on classical attacks against these systems, comparatively little work was done on quantum cryptanalysis itself, with a few papers in that direction from Inria teams on lattice-based problems [27], code-based problems [28], isogenies [29]. We will aim at characterizing the hardness of these problems for quantum computers in order to properly choose the security parameters required for different public key post-quantum schemes. Although symmetric cryptography appears less impacted by quantum computers, COSMIQ has shown that Grover's algorithm, as well as improved collision and k-list quantum algorithms, force us to modify the parameters of our block ciphers, operator modes and hash functions. We plan to continue studying the impact of quantum computers on the AES and SHA-3 functions [30], as well as

other designs currently proposed in another NIST competition devoted to lightweight cryptography.

Quantum cryptanalysis often relies on the same quantum tools: Grover's algorithm, quantum random walks, or quantum algorithms for the hidden subgroup problem. These algorithms are well studied in the literature but quantum cryptanalysis comes with new constraints since we are interested in realistic algorithms. A particular challenge for quantum cryptanalysis is evaluating the threat of machines that do not yet exist. This means that the community needs to agree on realistic cost models (and we plan to address this question by interacting with the other WP). In any case, we feel that both (standard) quantum memory and quantum random access memory (QRAM) will be very costly. We will therefore continue developing new tools for quantum cryptanalysis [31, 32] with a special focus on reducing the use of quantum memory and QRAM. We will also thrive to find applications of such generic algorithms to break a large spectrum of cryptosystems [29, 33, 34].

Security proofs form another important aspect of post-quantum cryptography: constructing a secure post-quantum primitive from a problem hard for quantum computers is nontrivial and design flaws can open the door to possible attacks. To avoid this, post-quantum primitives also require a quantum security proof. We will study these security proofs both for public key cryptography (especially the NIST candidates), in the quantum random oracle model or the plain model, continuing our existing work [35, 36], and will also extend these security proofs for symmetric cryptography.

We finally plan to exploit our knowledge in all aspects of quantum cryptanalysis to propose new designs for post-quantum cryptography, as we did for code-based cryptography [37, 38] and lightweight post-quantum symmetric cryptography [39]. Task T3.A will be undertaken by CASCADE and COSMIQ.

A relatively short-term objective is to understand how to exploit the first quantum processors that will become available in the coming years. Task T3.B is concerned with the development of algorithms for the NISQ era. The main applications concern optimization problems for which hybrid architectures are particularly relevant. Exploiting machine learning techniques, it is possible to train low-depth quantum circuits so as to optimize a particular functional. A specific objective of this task will be to develop NISQ-like algorithms for the cat qubits developed in WP1. This is a new subject for the Inria teams, but COSMIQ, MOCQUA and QUANTIC are motivated by studying these questions.

In T3.C, we will investigate how to integrate quantum computing with HPC. We indeed expect that the forthcoming quantum processors will ensure a tremendous acceleration of some specific applications but might not be well adapted to perform general-purpose processing. One option to enlarge the range of applications that quantum computing will be able to accelerate in that context consists in combining quantum with classical computing. This idea is not new and has shown to be very effective to popularize general-purpose computing on graphics processing units (GPGPU). A typical example is the significant acceleration of advanced linear algebra

algorithms by executing only matrix multiplications on GPU [40]. The subsequent hardware heterogeneity raises challenges both in terms of programming models and scheduling. A possible approach to handle them consists of abstracting the computation in terms of tasks and relying on a third-party software, often referred to as a runtime system, to which is delegated the burden of handling data consistency, scheduling decisions and data movements [41]. Of course, a QPU (Quantum Processing Unit) is not a GPU, the kernels it will accelerate most will differ and the physical interconnection between quantum and classical hardware remains extremely challenging, this is why this third task is considered as more prospective.

In an intermediate phase we can identify in HPC scientific libraries some specific tasks that could benefit to be delegated to a QPU. Another research track will concern the use of classical HPC ressources to deal with essential tasks in quantum computing. For instance it has been shown in [23] that the synthesis/compilation of quantum circuits can be significantly accelerated by adapting existing libraries like LAPACK or MAGMA and using GPUs. Three teams specialized in HPC, namely HiePACS, PARSYS and STORM accepted to join the consortium and the plan is to start exploring these questions with other relevant teams.

- **Interaction with other WP:** interaction with WP1 to understand realistic noise models and expected number of required physical qubits to run cryptanalysis; ideally the cat qubits engineered in WP1 will be exploited to demonstrate simple NISQ algorithms or proof-of-concepts; the integration of quantum accelerators with HPC is also related to the questions studied in WP2.

- **External funding/participants:** the ERCs of María Naya-Plasencia and Phong NGuyen are also centered around the theme of quantum cryptanalysis. Thomas Vidick (Caltech professor) obtained an Inria international chair and will participate to this WP. A CIFRE PhD thesis is currently shared by MOCQUA and EDF on quantum algorithms for optimisation problems.

Organization

- **Scientific meetings each semester** – We plan a scientific meeting every six months, where partners will present informally their work and where joint decisions (if any) will be addressed.
- **Workshops** – We plan to organize 2-3 focussed workshops during the project.
- **Meetings within the WP** – We also plan to hold regular meetings within the different work packages. These meetings which could take the form of (possibly online) seminars, reading groups or more general discussions will be essential to create a community and encourage collaborations between the different teams.
- **Requested resources** – The EQIP challenge does not involve much work for engineers and funding for PhD theses and postdocs is generally preferred:
  - 2-year postdoc for T1.A co-advised by MATHERIALS and QUANTIC
  - PhD for T1.B co-advised by CAGE and QUANTIC
  - PhD for T1.C co-advised by COSMIQ and QUANTIC: this thesis will also contribute to WP3
  - 2-year postdoc for T2.A co-advised by MOCQUA and DEDUCTEAM
  - 2-year engineer for T2.B co-advised by PACAP and MOCQUA
  - 2-year postdoc for T2.C co-advised by COSMIQ and GRACE
  - PhD for T2.D co-advised by DEDUCTEAM and PARSYS
  - PhD and 2-year postdoc for T3.A advised by CASCADE and COSMIQ
  - PhD for T3.B co-advised by COSMIQ, MOCQUA or QUANTIC
  - 2-year postdoc for T3.C co-advised by HiePACS, PARSYS or STORM.

Objectives for the 4 years

- Demonstration of error correction, as well as some protected gates, for cat qubits
- Mathematical/numerical model reduction methods for open quantum systems
- A versatile and well-founded high-level quantum language
- A public domain library of quantum routines for high-performance scientific computing
- An emulation platform for testing algorithms
- Methods and tools for optimizing fault-tolerant quantum computation
- Quantum cryptanalysis of symmetric and public-key cryptography

- NISQ compatible algorithms

Future possibilities (at the end of the Challenge)

There is currently a single project-team working at Inria full-time on quantum computing (QUANTIC) and 2 other teams with a critical mass on this subject (COSMIQ and MOCQUA). Moreover, collaboration between the different teams involved in the challenge has been limited in the past. A successful project will significantly enhance the level of discussions and collaboration within the institute and lead to the creation of new quantum project-teams.

References

[1] Frank Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019. 7

[2] Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A*, 86:032324, 2012. 7

[3] Zaki Leghtas, Gerhard Kirchmair, Brian Vlastakis, Robert J. Schoelkopf, Michel H. Devoret, and Mazyar Mirrahimi. Hardware-efficient autonomous quantum memory protection. *Phys. Rev. Lett.*, 111:120501, 2013. 7

[4] Mazyar Mirrahimi, Zaki Leghtas, Victor V Albert, Steven Touzard, Robert J Schoelkopf, Liang Jiang, and Michel H Devoret. Dynamically protected cat-qubits: a new paradigm for universal quantum computation. *New Journal of Physics*, 16(4):045014, 2014. 7

[5] Nissim Ofek et al. Extending the lifetime of a quantum bit with error correction in superconducting circuits. *Nature*, 536(7617):441–445, 2016. 7

[6] Z. Leghtas et al. Confining the state of light to a quantum manifold by engineered two-photon loss. *Science*, 347(6224):853–857, 2015. 7

[7] Raphaël Lescanne, Marius Villiers, Théau Peronnin, Alain Sarlette, Matthieu Delbecq, Benjamin Huard, Takis Kontos, Mazyar Mirrahimi, and Zaki Leghtas. Exponential suppression of bit-flips in a qubit encoded in an oscillator. *Nature Physics*, 2020. 7

[8] Jérémie Guillaud and Mazyar Mirrahimi. Repetition cat qubits for fault-tolerant quantum computation. *Phys. Rev. X*, 9:041053, 2019. 8

[9] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Phys. Rev. A*, 64:012310, 2001. 8

[10] P. Campagne-Ibarcq et al. A stabilized logical quantum bit encoded in grid states of a superconducting cavity. *arXiv preprint arXiv:1907.12487*, 2019. 8

[11] C. Le Bris and P. Rouchon. Low-rank numerical approximations for high-dimensional Lindblad equations. *Phys. Rev. A*, 87:022125, 2013. 8

[12] C. Le Bris, P. Rouchon, and J. Roussel. Adaptive low-rank approximation and denoised Monte Carlo approach for high-dimensional Lindblad equations. *Phys. Rev. A*, 92:062126, 2015. 8

[13] M. V. Berry. Transitionless quantum driving. *Journal of Physics A: Mathematical and Theoretical*, 42(36):365303, 2009. 8

[14] Alexander S Green, Peter LeFanu Lumsdaine, Neil J Ross, Peter Selinger, and Benoît Valiron. Quipper: a scalable quantum programming language. In *Proceedings of the 34th ACM SIGPLAN conference on Programming language design and implementation*, pages 333–342, 2013. 10

[15] Peter Selinger, Benoıt Valiron, et al. Quantum lambda calculus. *Semantic techniques in quantum computation*, pages 135–172, 2009. 10

[16] Gilles Dowek and Pablo Arrighi. Lineal: A linear-algebraic lambda-calculus. *Logical Methods in Computer Science*, 13, 2017. 10

[17] Jean-Pierre Tillich and Gilles Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2014. 10

[18] Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zémor. Quantum expander codes. In *Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on*, pages 810–824. IEEE, 2015. 10

[19] Omar Fawzi, Antoine Grospellier, and Anthony Leverrier. Constant overhead quantum fault-tolerance with quantum expander codes. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 743–754. IEEE, 2018. 10

[20] Ross Duncan, Aleks Kissinger, Simon Pedrix, and John Van De Wetering. Graph-theoretic Simplification of Quantum Circuits with the ZX-calculus. *arXiv preprint arXiv:1902.03178*, 2019. 10

[21] Marcos Yukio Siraichi, Vinicius Fernandes dos Santos, Caroline Collange, and Fernando Magno Quintão Pereira. Qubit allocation as a combination of subgraph isomorphism and token swapping. In *OOPSLA*, Athens, Greece, 2019. 10

[22] Timothée Goubault de Brugiere and Marc Baboulin and Benoit Valiron and Cyril Allouche. Synthesizing quantum circuits via numerical optimization. In *Computational Science - ICCS 2019 - 19th International Conference, Faro, Portugal, June 12-14, 2019, Proceedings, Part II*, volume 11537 of *Lecture Notes in Computer Science*, pages 3–16. Springer, 2019. 10

[23] Timothee Goubault de Brugiere and Marc Baboulin and Benoit Valiron and Cyril Allouche. Quantum circuits synthesis using householder transformations. *Comput. Phys. Commun.*, 248:107001, 2020. 10, 14

[24] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+ T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 559–568, 2018. 10

[25] Simon Perdrix. Quantum entanglement analysis based on abstract interpretation. In *International Static Analysis Symposium*, pages 270–282. Springer, 2008. 10

[26] Daniel E Browne, Elham Kashefi, Mehdi Mhalla, and Simon Perdrix. Generalized flow and determinism in measurement-based quantum computation. *New Journal of Physics*, 9(8):250–250, 2007. 10

[27] Yoshinori Aono, Phong Q. Nguyen, and Yixin Shen. Quantum lattice enumeration and tweaking discrete pruning. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 405–434. Springer, 2018. 12

[28] Ghazal Kachigar and Jean-Pierre Tillich. Quantum information set decoding algorithms. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings*, volume 10346 of *Lecture Notes in Computer Science*, pages 69–89. Springer, 2017. 12

[29] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of CSIDH and ordinary isogeny-based schemes. *IACR Cryptology ePrint Archive*, 2018:537, 2018. 12, 13

[30] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. Quantum security analysis of AES. *IACR Trans. Symmetric Cryptol.*, 2019(2):55–93, 2019. 12

[31] André Chailloux, María Naya-Plasencia, and André Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 211–240. Springer, 2017. 13

[32] Xavier Bonnetain, Rémi Bricout, André Schrottenloher, and Yixin Shen. Improved classical and quantum algorithms for subset-sum. *IACR Cryptology ePrint Archive*, 2020:168, 2020. 13

[33] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237. Springer, 2016. 13

[34] Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher. Quantum attacks without superposition queries: The offline simon's algorithm. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of*

Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I, volume 11921 of *Lecture Notes in Computer Science*, pages 552–583. Springer, 2019. 13

[35] André Chailloux. Quantum security of the Fiat-Shamir transform of commit and open protocols. *IACR Cryptology ePrint Archive*, 2019:699, 2019. 13

[36] André Chailloux and Thomas Debris-Alazard. Tight and optimal reductions for signatures based on average trapdoor preimage sampleable functions and applications to code-based signatures. *IACR Cryptology ePrint Archive*, 2020:6, 2020. 13

[37] Nicolas Aragon et al. BIKE: Bit Flipping Key Encapsulation, 2017. Submission to the NIST post quantum standardization process. 13

[38] Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich. Wave: A new family of trapdoor one-way preimage sampleable functions based on codes. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 21–51. Springer, 2019. 13

[39] Anne Canteaut, Sébastien Duval, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Thomas Pornin, and André Schrottenloher. Saturnin: a suite of lightweight symmetric algorithms for post-quantum security, 2019. Soumission à la compétition "Lightweight Cryptography" du NIST. 13

[40] Emmanuel Agullo, Jim Demmel, Jack Dongarra, Bilel Hadri, Jakub Kurzak, Julien Langou, Hatem Ltaief, Piotr Luszczek, and Stanimire Tomov. Numerical linear algebra on emerging architectures: The plasma and magma projects. In *Journal of Physics: Conference Series*, volume 180, page 012037. IOP Publishing, 2009. 14

[41] Cédric Augonnet, Samuel Thibault, Raymond Namyst, and Pierre-André Wacrenier. Starpu: a unified platform for task scheduling on heterogeneous multicore architectures. *Concurrency and Computation: Practice and Experience*, 23(2):187–198, 2011. 14