SORBONNE UNIVERSITÉ

PROGRAMME INSTITUTS ET INITIATIVES

Appel à projet – campagne 2021

Proposition de projet de recherche doctoral (PRD)

QICS - Quantum Information Center Sorbonne

Intitulé du projet de recherche doctoral (PRD): Impact of quantum computers on Impagliazzo's five worlds

Directrice ou directeur de thèse porteuse ou porteur du projet (titulaire d'une HDR) :

NOM : **Vergnaud** Prénom : **Damien**

Titre : Chargé de Recherche ou

e-mail : damien.vergnaud@lip6.fr

Adresse professionnelle : *(site, adresse, bât., bureau)* Couloir 26-00, Étage 1, Bureau 101b
4 place Jussieu
75252 PARIS CEDEX 05
FRANCE

Unité de Recherche :

Intitulé : LIP6

Code *(ex. UMR xxxx)* : UMR 7606

École Doctorale de rattachement de l'équipe (future école doctorale de la doctorante ou du doctorant) : ED130-EDITE

Doctorantes et doctorants actuellement encadrés par la directrice ou le directeur de thèse (préciser le nombre de doctorantes ou doctorants, leur année de 1e inscription et la quotité d'encadrement) :

2 doctorant.e.s encadré.e.s

Florette Martinez - 2019

Abdul Rahman Taleb - 2020

Co-encadrante ou co-encadrant :

NOM : **Bredariol Grilo** Prénom : **Alex**

Titre : Chargé de Recherche ou HDR ☐

e-mail : Alex.Bredariol-Grilo@lip6.fr

Unité de Recherche :
Intitulé : LIP6
Code *(ex. UMR xxxx)* : UMR 7606

École Doctorale de rattachement : Choisissez un élément :
Ou si ED non Alliance SU :

Doctorantes et doctorants actuellement encadrés par la directrice ou le directeur de thèse (préciser le nombre de doctorantes ou doctorants, leur année de 1e inscription et la quotité d'encadrement) :

0 doctorant.e.s encadré.e.s

Co-encadrante ou co-encadrant :

NOM : Prénom :
Titre : Choisissez un élément : ou HDR ☐
e-mail :

Unité de Recherche :
Intitulé :
Code *(ex. UMR xxxx)* :

École Doctorale de rattachement : Choisissez un élément :
Ou si ED non Alliance SU :

Doctorantes et doctorants actuellement encadrés par la directrice ou le directeur de thèse (préciser le nombre de doctorantes ou doctorants, leur année de 1e inscription et la quotité d'encadrement) :

Cotutelle internationale : ☐ Non ☐ Oui, précisez Pays et Université :

Selon vous, ce projet est-il susceptible d'intéresser une autre Initiative ou un autre Institut ?
☐ Non ☐ Oui, précisez Choisissez l'institut ou l'initiative :

SORBONNE UNIVERSITÉ

Description du projet de recherche doctoral *(en français ou en anglais)* :

Ce texte sera diffusé en ligne : il ne doit pas excéder 3 pages et est écrit en interligne simple.

Détailler le contexte, l'objectif scientifique, la justification de l'approche scientifique ainsi que l'adéquation à l'initiative/l'Institut.

Le cas échéant, préciser le rôle de chaque encadrant ainsi que les compétences scientifiques apportées. Indiquer les publications/productions des encadrants en lien avec le projet.
Préciser le profil d'étudiant(e) recherché.

Background

Since its early stages, quantum computing has had drastic consequences to cryptography. In the one hand, (full-scalable) quantum computers could be used to break widely used cryptosystems, given the celebrated Shor's algorithm for factoring. On the other hand, quantum resources have also been used to realize cryptographic tasks that are otherwise impossible, for example quantum money (e.g. Wiesner'80), sharing private keys (e.g. Bennet and Brassard'84) or generating certifiable randomness (e.g. Colbeck'09). We remark that all of these primitives can be constructed in the quantum world unconditionally, meaning that we do not need to impose any computational assumption on the adversaries.

These results raise an ambitious possibility for the field of cryptography, namely the possibility of realizing every cryptographic primitive unconditionally with quantum resources.
Unfortunately, this was shown impossible, we know today several primitives that are not realizable even with quantum resources unconditionally (Mayers'97, Lo and Chau'97). Therefore, in order to be able to implement cryptographic protocols of interest, even in a quantum world, we must rely on computational assumptions.

We have seen that these computational assumptions come in two flavours. First, we see constructions based on the hardness of specific problems, such as factoring, lattices problems, etc. As spotted by Shor's algorithm, the downside of this approach is that we are walking on thin ice by relying on particular assumptions and this brings us to the second, and more general, way of constructing cryptographic schemes. This second perspective in cryptography is to rely on the hardness of abstract problems with special properties. For example, we know how to construct some protocols based on the existence of one-way functions (OWF), which are functions that are

easy to compute and hard to invert. We remark that these protocols work for any OWF that you might implement.

Of course, we still have the problem to show that these generic objects such as OWFs exist and to structure this, Impagliazzo proposed five possible “worlds” in which we might be living:

- Algorithmica: P = NP or something "morally equivalent" like fast probabilistic algorithms for NP.
- Heuristica: NP problems are hard in the worst case but easy on average.
- Pessiland: NP problems are hard on average but no one-way functions exist. We can easily create hard NP problems, but not hard NP problems where we know the solution.
- Minicrypt: One-way functions exist
- Cryptomania: Public-key cryptography (PKE) is possible, i.e. parties can exchange secrets over open channels.

Recently, a sixth world was later added with stronger cryptographic primitives than PKE.

- Obfutopia: Obfuscation of programs is possible

The first three worlds are not so interesting for cryptography (using our current security notions), since they actually say that cryptography is not possible. Then, there has been a lot of study on trying to understand which primitives are possible in Minicrypt, Cryptomania and Obfutopia. More concretely, there has been a lot of study on the (im)possibilities of implementation of cryptographic primitives with minimal set of assumptions.

Recently, Grilo et al.’20 and Bartusek et al.’20 have independently proved that oblivious transfer can be built from OWF in the quantum world, which was an open problem since the protocol proposal of Bennet et al ‘96.(Roughly, in oblivious transfer, Alice has two messages m0 and m1 and Bob has a bit b. At the end of the protocol, Alice does not learn b and Bob learns mb, but not mb). These results are another example where quantum resources can help us implement cryptographic primitives from weaker assumptions, since there are strong indications that OT cannot be built from OWF in the classical world.

PhD project

The main goal in our project is to explore novel consequences that quantum computing could bring to Impagliazzo's 5 worlds, specially its impact on cryptography. Despite the impressive success of quantum computation/cryptography, we remark that progress on this line has been very limited. Examples of questions that could be explored by the PhD candidate are:

Constant-round ZK proofs from OWF: There is strong evidence that zero-knowledge proofs (a fundamental cryptographic primitive) cannot be implemented in constant-round classically in the plain mode, i.e. without any trusted help (Katz'08). However, these no-go results rely on complexity theoretical assumptions that do not quantize. Thus, a natural open question that could be explore in this PhD project is the (in)feasibility of constant-round quantum zero-knowledge proofs (ideally from one-way functions). This could clarify which type of advantage quantum resources can provide on the construction of cryptographic primitives.

Role of quantum obfuscation in quantum cryptography: In the classical world, the concept of indistinguishable obfuscation (iO), which asks that the ofuscation of two programs with the same functionality cannot be distinguished, has been shown to be a very strong primitive that can enable the implementation of several cryptographic primitives which are not known to exist otherwise. To stress its usefulness, iO is frequently called "crypto-complete" in the classical scenario. Such a strong functionality comes of course with a cost: for decades the existence of secure iO schemes

was elusive, until a very recent result of Jain, Lin and Sahai, which constructs iO from well-founded cryptographic assumptions.

The study of obfuscation in the quantum setting, specially its consequences, has been very limited. In particular, a direction that could be pursued in this PhD project would be to study the feasibility of strong quantum functionalities from quantum iO.

Lower bounds on quantum cryptographic protocols. Shoup'97 showed that in a "generic group" model, it is impossible to solve the discrete logarithm problem (or Diffie-Hellman) of a group of prime order p using O(sqrt(p)) group operations. Shor's polynomial algorithm for discrete-log directly implies that such a lower bound does not hold in the quantum setting. One potential direction for this PhD project would be to study if such lower bounds on the computational complexity for quantum algorithms can be proven for other generic mathematical structures, for example the Couveignes hard homogeneous spaces (based on group actions) underlying the cryptographic constructions based on elliptic curves isogenies, a cryptographic assumption that has resisted to quantum attacks (so far).

Pertinence of the project

This PhD concerns topics in the theoretical aspects (post-)quantum cryptography, a very important subject within the scope of QICS. The different background of both PhD supervisors (cryptography for D. Vergnaud and quantum computing for A. Grilo) combine in a very natural way to supervise this project. We list now some publications from the supervisors that are relevant for this proposal:

Grilo, Lin, Song, and Vaikuntanathan. Oblivious Transfer is in MiniQCrypt. Accepted at Eurocrypt 2021 and plenary talk at QIP 2021.

*Alagic, Childs, **Grilo** and Hung. Non-interactive Classical Verification of Quantum Computation. TCC 2020 and contributed talk at QIP 2021.*

*Broadbent and **Grilo.** QMA-hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge, FOCS 2020 and plenary talk at QIP 2021*

Merci d'enregistrer votre fichier au format PDF et de le nommer :
«ACRONYME de l'initiative/institut – AAP 2021 – NOM Porteur.euse Projet »

Fichier envoyer simultanément par e-mail à l'ED de rattachement et au programme :
cd_instituts_et_initiatives@listes.upmc.fr avant le 20 février.