www.snf.ch
Wildhainweg 3, Postfach 8232, CH-3001 Bern

Application form mySNF

Instrument **Bridge - Discovery**

Part 1: General Information

Basic data

Project Title	Self-testing Quantum Random Number Generator
Project title in English	Self-testing Quantum Random Number Generator

Research Field	Engineering sciences
Main Discipline	20508 Microelectronics. Optoelectronics
Field of the planned innovation	Optoelectronic / photonic components and systems
University	Université de Genève - GE

Applicant(s)

Main Applicant	**Hugo Zbinden**
Other applicant(s)	Etienne Messerli
	Nicolas Brunner

Grant Application

Amount requested (CHF)	Total	**798'538**
Requested starting date	**01.12.2017**	
Duration (months)	**24**	

Attachments

Project description	ProjectPart_Zbinden.pdf
Curriculum vitae	CV_Zbinden.pdf
	CV_Messerli_ang.pdf
	CV_Brunner.pdf
Other annexes	SupportLetter_IDQuantique.pdf
	Annexe_1-Utilisation_des_Rsultats_entre_Partenaires_de_Projet_v05.pdf

BRIDGE

Discovery

Project description

Self-testing Quantum Random Number Generator

FNSNF
Swiss National Science Foundation

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
Commission for Technology and Innovation CTI
Innovation Promotion Agency

1. Summary

The generation of random numbers plays a crucial role in many applications in science and technology, in particular for simulation and cryptography. It is of fundamental importance that the generated numbers are truly random, as any deviation may jeopardize security. Notably, recent breaches of cryptographic protocols have exploited weaknesses in the random number generation. In this context, schemes exploiting the inherent randomness of quantum physics have been extensively investigated. Quantum random number generation (QRNG) devices are now commercially available, which arguably represents one of the most successful developments of quantum technologies so far.

Despite this success, recent developments have pinpointed a general weakness and limitation of standard QRNG devices (including all commercial ones). Specifically, these devices fail to provide an accurate estimate of the entropy (i.e. quantifying how much randomness is generated in the quantum process). This has been recognized as a crucial issue for QRNG, since a poor entropy estimate may open security breaches. In practice it is usually challenging to accurately estimate entropy, since the implementation of any QRNG device is prone to unavoidable technical imperfections that lead to noise. How can one differentiate this noise from true quantum randomness? Even more importantly, the performance of a QRNG device may degrade over time. If the device malfunctions (or even breaks), low quality randomness (or even no randomness at all) is generated without the user being aware of it.

Recently, we have proposed a promising solution for addressing the above problems, by developing a “self-testing” QRNG scheme. Here, the user can operate the QRNG device while simultaneously testing it, and thus certify the continuous generation of truly random numbers. Specifically, the generator can quantify the amount of quantum entropy generated by the system in real time, and unambiguously separate it from technical noise. This scheme combines strong security and ease of implementation, as we demonstrated in a proof-of-principle experiment, achieving randomness generation rates comparable to commercial QRNGs (~10 MHz). The main objective of the present project is to develop a demonstrator for self-testing QRNG. This demonstrator should be compact, simple to use, and achieve high rates. Importantly it should comprise only standard optical and electronic components, in order to ensure low cost. In turn, the demonstrator will place us in an ideal position for approaching industrial partners, and thus to potentially launch the commercial development of self-testing QRNG. On the scientific level, the project will bridge the gap between abstract device-independent quantum information processing and commercial quantum technology.

2. Project description

2.1 Current state of research in the field

Many tasks in modern science and technology make use of random numbers, including Monte Carlo simulation, statistical sampling, cryptography, and gaming applications [Haye01]. Ideally a random number generator should produce a chain of bits with high entropy at a high rate. By high entropy, it is meant that nobody can predict the value of the bit before it is revealed. Entropy should thus be understood as a measure of randomness. This represents a key requirement for data encryption. Indeed, for all commonly employed cryptographic protocols (such as DSA and RSA), as well as for quantum cryptography, it is crucial that the key (i.e. in the random sequence used as seed) is random. Currently, most keys are generated by arithmetic approaches and are thus only pseudo-random. However, as John von Neumann said in 1951: "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin." Indeed, most recent breaches of cryptographic protocols have exploited weaknesses in the random number generation [LHAB12, Mark14].

It turns out that quantum systems are well suited for the task of generating truly random numbers. This is due to the inherent randomness in quantum physics. In recent years, an intense effort has been devoted to realize quantum random number generation (QRNG) devices (see e.g. [BAKM16, HeGa17]), which are now commercially available [Idqu17]. Arguably this represents one of the most successful developments of quantum technologies so far.

A QRNG device can be implemented in a simple setup, exploiting the inherent randomness in a quantum measurement. For example, one may send a single photon onto a balanced beam splitter and detect the output path [RaOT94, JAWW00, SGGG00]. Other variants measure the arrival time of single photons [StRo07, DYSS08, WLBR11, NZZW14], the phase noise of a laser [UAIH08, QCLQ10, AAJC14], vacuum fluctuations [GWSD10, SyAL11], and shot-noise in mobile phone cameras [SMZG14].

In theory, any of the above QRNG scheme can generate perfect randomness. In practice however, their implementation is prone to unavoidable technical imperfections that generate noise. Certifying genuine quantum randomness in such a setting becomes a challenging problem. This is because one should now distinguish true quantum randomness from technical noise. Indeed, an adversary may have partial knowledge (or even control) over the processes generating technical noise, and thus be able to guess the output bits. Hence it is crucial to accurately estimate how much quantum entropy is generated by a given QRNG device, and unambiguously separate this from fluctuations due to technical noise. This requires a precise theoretical modelling of the QRNG device [FrRT13, MXXT13], which is usually a cumbersome task. Indeed, giving a faithful mathematical description of a real device, including all its potential technical imperfections, is challenging. A further limitation comes from the fact that the properties of the device may change during its lifetime. In particular, if the device malfunctions, or even breaks, low quality randomness is generated without the user being aware of it. In all the above cases an incorrect estimation of the

amount of entropy will lead to the generation of low quality randomness (or even no randomness at all), and thus potentially compromise security of a cryptographic protocol.

It turns out that these problems can be circumvented via the so-called device-independent (DI) approach to randomness generation. Here the presence of genuine quantum randomness can be guaranteed based on the effect of quantum nonlocality [Col07, PAMG10]; see [AcMa16] for a recent review. Specifically, the observation of quantum nonlocality (that is, experimental statistics violating a Bell inequality), implies that the entropy of the output data can be certified in a black-box scenario [CoRe11]. That is, no detailed knowledge of the physical implementation is required for certifying entropy; observed data is enough. This provides a highly reliable and secure form of randomness certification. Indeed, since the devices do not need to be precisely characterized (and could in principle be completely untrusted), the method is robust against technical imperfections. However, implementing DI quantum randomness generation is extremely challenging, as the protocol requires the observation of a genuine (loophole-free) Bell inequality violation. This was achieved recently in proof-of-principle experiments [PAMG10, CMAC13] using state-of-the-art experimental setups. However, the reported randomness generation rates were extremely low (a few bits per hour). Therefore, the possibility of a commercial DI QRNG device seems extremely unlikely in the near future. Moreover, it is unclear whether the full DI security level is actually required for a practical, reliable and secure QRNG device.

More recently, a novel approach termed semi-DI has been proposed [PaBr11]. This represents an intermediate solution between the fully DI scenario and the standard "device-dependent" approach. It thus explores the trade-off between ease of implementation and strong DI security. Specifically, the semi-DI approach considers a prepare-and-measure setup (hence avoiding the complication of a Bell inequality test experiment). By adding a partial level of trust in the devices, strong security can still be obtained. Usually, semi-DI randomness generation protocols assume that the quantum systems have bounded dimension [LYWZ11, LPYG12, BoQB14, WoPi15]. Hence these schemes require only general assumptions about the physical implementation, but no detailed characterisation of the devices. Experimental demonstrations have been reported [CCGB14, LBLL15, MTHM16]. Alternative approaches based on trusted measurement devices [VMTV14, CZYM16, XuSW16, MaVV17], or a trusted source [CaZM15], have been reported. While significant progress has been achieved, it is fair to say that none of these approaches achieves the optimal balance between simplicity, performance, and security.

2.2 Own achievements in the field

The consortium has a strong and broad expertise in the area of quantum random number generation. Hugo Zbinden pioneered the experimental development of QRNGs which subsequently led to the first commercial product marketed by the SME IdQuantique, currently world-leader in this area. Nicolas Brunner developed DI and semi-DI quantum information processing. Recent collaborations between the Zbinden and Brunner groups have led to simple and efficient semi-DI QRNG protocols, and their experimental demonstration. In parallel, the group of Messerli has developed strong expertise in the domain of high performance data treatment with reconfigurable embedded digital circuit. Collaboration between the Zbinden and Messerli groups started with the nano-tera QCrypt

project in 2010 and now continues with an Interreg project (Easy-phi). In the following, we describe recent achievements of the groups in more detail, as well as preliminary undertakings relevant to the project.

The Department of Applied Physics at the University of Geneva pioneered the development of QRNGs, and has since then remained at the forefront of research in this area. Specifically, the groups led by Hugo Zbinden and Nicolas Gisin reported the first implementation of a QRNG [SGGG00]. The latter was based on single photons sent to a balanced (50/50) beam-splitter followed by two single-photon detectors. According to quantum theory, which detector will click is unpredictable, and thus a random event. This proof-of-principle experiment served as a basis for the design of a commercial product marketed by the newly created start-up company IdQuantique. This commercial QRNG arguably represents one of the most successful products developed by the company [Idqu17], which has remained world-leader in this area ever since.

More recently, the Zbinden group developed a novel approach to QRNG based on the multi-pixel cameras [SMZG14], which are nowadays featured on any cell phone. This represents an important step, as it makes quantum random number generation accessible to a much wider range of users in principle. The main idea is to exploit the unpredictable fluctuations (shot noise) in the number of photons detected on any pixel of the camera in order to extract randomness. This discovery has given rise to a patent (EP2940923 A1 / US20170060534 A1), and very recently, to a smartphone application freely available on the internet.

On the theoretical side, the Brunner group has developed strong expertise in DI and semi-DI quantum information processing. In particular, Nicolas Brunner pioneered the development of DI quantum cryptography [ABGM07] and proposed semi-DI quantum cryptography [PaBr11]. Since 2012, the Brunner group has developed a research activity towards first experimental demonstrations of DI and semi-DI QRNGs, in particular by developing experimentally friendly protocols. In 2013, the group provided theoretical support for the first demonstration of DI QRNG in a photonic setup [CMAC13], achieved in the group of Paul Kwiat (Univ. of Illinois). In 2014, the group started a fruitful collaboration with the Zbinden group at UNIGE, developing practical and secure semi-DI solutions for QRNGs. This resulted in the first proof-of-principle experiment of semi-DI QRNG [LBLL15]. The main limitation of this first experiment was its low randomness generation rate (0.04 bits/sec) and the complexity of the setup.

In parallel, the Messerli group has developed expertise in the domain of high performance data treatment with reconfigurable, embedded, digital circuits. In particular, this includes Field Programmable Gate Arrays (FPGAs), Graphical Processing Units (GPUs), and Central Processing Units (CPUs). Recently, the group has implemented means for automatic real-time performance analysis of algorithms in order to identify the best technology amongst FPGA, GPU, or CPU for given code [REDS1]. The group also has extensive experience with high-speed electronics [REDS3] and parallel processing using System on Chip with a FPGA (SoC-FPGA). The group is also active in health research, in particular for human genome encoding and compression via multiple parallel FPGAs [REDS2].

The Messerli group has collaborated with the Zbinden group on quantum technology projects. The first collaboration was within the Nano-tera project QCrypt [REDS3]. More recently, a common project Interreg "France-Suisse" is underway. This project entitled "Easy-phi" aims to provide an open hardware, modular, generic, and collaborative scientific instrumentation platform.

Preliminary undertakings for the present project

Recently, the Brunner and Zbinden groups developed a novel protocol for semi-DI randomness generation, which is the foundation for the present project. Based on a completely new theoretical approach, this protocol combines ease-of-implementation, high rate, and strong security. It thus clearly outperforms previous semi-DI schemes, and represents a promising solution for a practical semi-DI QRNG. We implemented the protocol in a proof-of-principle experiment, reporting randomness generation rates on the order of 10 Mbits/sec, comparable to commercial QRNGs. These results (protocol + experiment) were reported in a scientific article just accepted for publication in Physical Review Applied [BMEH16]. In parallel, a patent application has been filed in October 2016 [PAT].

The main feature of our QRNG is that it is "self-testing". That is, the user can operate the QRNG device while simultaneously testing it, thus certifying the continuous generation of truly random numbers. Specifically, the test performed by the user allows him to quantify the amount of quantum entropy generated by the system, which can be estimated based only on the observed data. In this way, quantum entropy is separated from technical noise. The protocol and the basic setup are illustrated in Figure 1. The protocol consists in three steps:

(1) Data collection from measurements on quantum states.
(2) Estimation of the genuinely quantum entropy in the data.
(3) Randomness extraction resulting in a perfectly random output bit string.

In step (1), a quantum system is prepared in one out of two possible non-orthogonal quantum states. According to quantum theory, the two states can thus not be distinguished with certainty. However, by performing unambiguous state discrimination (USD), the two states can be unambiguously distinguished (i.e. without false positives), at the price of having a certain minimal rate of inconclusive events. The occurrence of these inconclusive events must be genuinely random (if not, the two states could be distinguished better), and this is the source of quantum randomness that the QRNG uses. Importantly, the amount of randomness can be directly quantified from the observed experimental data. This is achieved in step (2), based on the theoretical methods we developed in [BMEH16]. Finally, in step (3), a string of perfectly random bits can be obtained from the raw data via the procedure of randomness extraction. Importantly, the entropy estimate achieved in step (2) is crucial for the randomness extraction, as it determines the compression factor to obtain the final perfectly random output bit string.

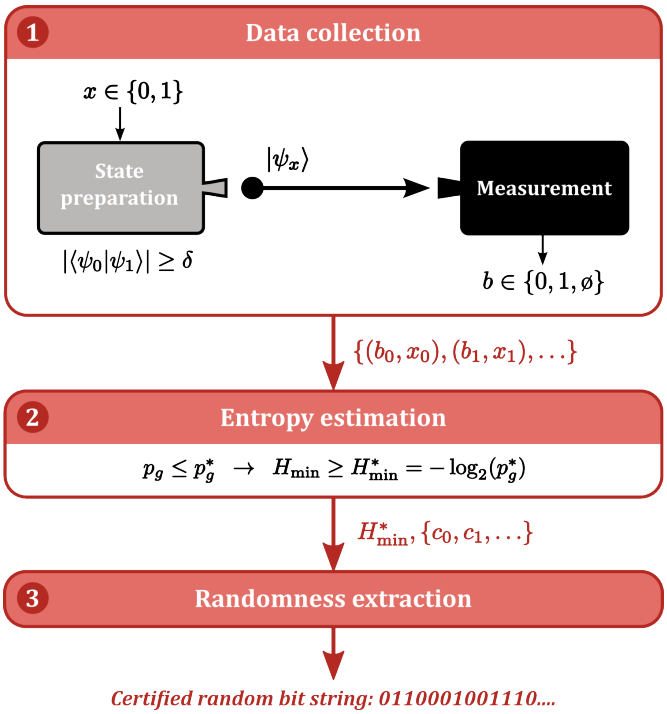


Figure 1: Schematic of the self- testing QRNG protocol. In step 1 of the protocol, a state preparation device receives a binary input x, produced e.g. by pseudo random number generation, and prepares one of two non-orthogonal quantum states. The state is sent to a measurement device, which measures and produces a ternary output b. This process is iterated to produce a series of pairs (b,x) of outputs and inputs, which constitutes the raw data produced by the QRNG. In each iteration, the overlap of the two quantum states is lower bounded by their overlap δ, which implies that they cannot be perfectly distinguished. In step 2, a raw bit string is produced from the outputs, defining c to be 0 or 1 if the measurement was conclusive or inconclusive, respectively. That is, if the output b is 0,1 or ø respectively. Then, crucially, a bound on the min-entropy H_{min} in this bit string is established based on the raw data, and knowledge of δ. Finally, the raw bit string and the entropy bound is passed to a randomness extractor, which extracts a final (shorter) string of certified, perfectly random bits.

2.3 Scientific contents

This project will build upon the novel concept for a self-testing QRNG recently developed by the Brunner and Zbinden groups, as described above. The protocol allows the user to continuously monitor the quantum entropy generated by the system and hence certify genuine randomness in real time. Our recent proof-of-principle experiment [BMEH16] demonstrated the strong potential of this approach to combine high security and ease of implementation, and in particular we reported random bit rates of ~10 Mbits/sec, comparable to commercial QRNGs but with significantly enhanced security. Our scheme thus appears as a very promising solution for a practical solution for semi-DI QRNG. However, important challenges must still be addressed before potential commercial partners can be approached. The randomness generation rate can be increased further, and an efficient, economical design using commercially available optics and electronics should be

identified, encompassing both the quantum measurement and the post-processing randomness extraction. This is precisely the goal of the present BRIDGE project.

The main objective of the present application is to develop a demonstrator for our semi-DI QRNG. This demonstrator should be compact, simple to use, and achieve high rates. Importantly it should comprise only standard optical and electronic components, in order to ensure low-cost.

The demonstrator will combine a laser source, single-photon detection, and control and post-processing electronics, as sketched in Fig. 2. The laser prepares weak coherent light pulses, which encode non-orthogonal quantum states whose overlap can be controlled by adjusting the intensity of the emitted light. An unambiguous state discrimination measurement is implemented by detecting the light pulses on a single-photon detector. Control electronics regulates this process and collects the raw data, which is passed on to post-processing electronics, which performs an estimate of the entropy and implements randomness extraction, to produce a perfectly random output bit string.

To achieve our target of a system which is simple to operate and can compete on bit rates with commercial QRNGs while maintaining strong security, both the theoretical security analysis, as well as the optical and electronic parts of the device must be optimised. Specifically, we target the following characteristics for the demonstrator:

- High randomness rate: 100 Mbits/sec (clock system: 250 MHz)
- Compactness: size (LWH): 200 x 100 x 40 mm
- Plug-n-play: USB & Ethernet output connection
- Low power consumption: 250 W
- Reliability: tolerated deviation from a perfect random sequence: < 10^-9

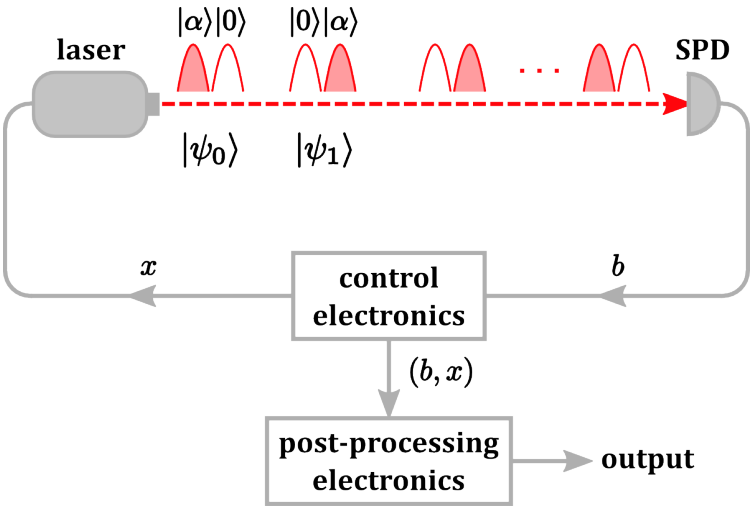


Figure 2: Schematic of the structure of the demonstrator. For each round of data collection, the control electronics pseudo-randomly generates the variable x which determines the state generated by the laser and records the output b of the single photon detector (SPD). All this information is sent to the post-processing electronics which estimates the amount of entropy in the raw data and performs randomness extraction to output a perfectly random bit string. Note that, to achieve a high throughput, the electronics will be based on an FPGA.

Achieving these features will ensure that our demonstrator combines strong self-testing security while maintaining an overall performance comparable to existing commercial QRNGs. In order to realize the envisaged demonstrator, we have identified a list of intermediate and more specific objectives. Our proposal is structured along three main research lines, which are strongly interconnected.

1. **Security analysis.** Here we aim to provide an improved characterization of the theoretical analysis of the self-testing protocol. A first goal will be to determine the optimal trade-off between security and ease of implementation. In parallel we will identify the optimal solution for randomness extraction, based on performance and limitations of available electronic processing devices (e.g. FPGAs). Finally, we will explore the potential of our self-testing approach for more general quantum information processing tasks, in particular quantum cryptography.

2. **Conception of the demonstrator.** We will characterize the available electrical and optical components. More specifically, the choice of data processing components will be in accordance with the needs of computing capabilities defined in point 1. The choice will be validated using development kits and the corresponding firmware will be developed. Based on this, we will choose the best components for implementing the demonstrator. The latter should be compact, simple to operate, achieve high rates (>10 MHz), and low-cost.

3. **Realisation and test of the demonstrator.** This last part will be dedicated to the integration of all the elements, i.e. optics, controlling electronics, and data post-processing units, in a single platform. Electronic boards will be developed to achieve the above specifications. The project will end with the characterisation of the generator in term of performance, robustness to the external condition, and stability over time. This step will validate our approach for the realisation of a future commercial device.

The project requires a wide range of expertise. Security aspects and methods for randomness certification demand expertise in quantum information theory (Brunner group). The experimental realisation of the self-testing QRNG requires strong expertise in quantum optics and experimental aspects of quantum information (Zbinden group). Finally, the implementation of a plug-and-play demonstrator, with features comparable to the commercial QRNGs, requires expertise in the area of fast and integrated electronics (Messerli group). This justifies a consortium involving the three groups mentioned above.

Scientific Impact

This project will have a strong impact on the fields of quantum random number generation in particular, and quantum information science in general. Device-independent quantum information processing holds great promise for unprecedented security and robustness to imperfections in implementation, but progress so far has mainly been theoretical, due to the technological challenges involved in real-world realisations. Device-dependent QRNG on the other hand is currently one of the most advanced quantum technologies in practice.

By developing self-testing QRNG from the proof-of-principle stage to a practically viable technology, the present project will bridge the gap between recent theoretical progress on DI randomness generation and commercial "device-dependent" QRNG systems. This will give a strong impulse to the new and promising semi-DI approach to quantum information processing and bring semi-DI QRNG to full fruition. It is likely to motivate future advances linking fully device-independent and device-dependent quantum information protocols, both theoretically and experimentally. Furthermore, the project will open for a practical and realistic exploration of the trade-off between security and ease-of-implementation in QRNG, which may potentially give rise to new breakthroughs in what is already one of leading applications of quantum technology.

Moreover, the dedicated randomness-extraction platform envisaged in the project may find additional applications in other implementations of QRNG and possibly classical RNG. We also note that randomness extraction is strongly linked to privacy amplification, which is fundamental for quantum key distribution protocols and thus further applications may be expected for quantum communication and technologies.

To maximize the scientific impact, the results will be disseminated by publication in international peer-reviewed journals, and by presentations at international conferences and workshops on quantum information science and technologies.

2.4 Innovative potential

The generation of random numbers is central to many applications. For cryptographic protocols, it is crucial that the key is truly random, as any failure opens potential loopholes. Notably, recent breaches of cryptographic protocols have exploited weaknesses in the random number generation [LHAB12, Bell08]. The use of quantum devices brought considerable improvement in this context. Commercial QRNGs have been available for more than 10 years, and there is still an intense research effort towards developing faster and more reliable devices.

However, the problem of accurate entropy estimation, i.e. quantifying how much randomness is generated in some quantum process, has been recognized as a crucial issue, as poor entropy characterization may open important security breaches. This clearly stands out as one of the main challenges in randomness generation today. Therefore, our vision of developing a practical "self-testing" QRNG is timely and may pave the way towards the next generation of QRNGs.

Moreover, our project will also have significant technological impact. The know-how developed during the project will benefit the areas of single-photon detection and high-speed electronics.

Our demonstrator will require single-photon detectors with high performance, in particular fast detection rates and low dead time, combined with high-speed electronics. The resulting fast and efficient single-photon detection could find use in quantum information science, as well as many other domains such as medicine or astrophysics.

In parallel, we will develop compact and efficient solutions for randomness extraction. This type of data post-processing could lead to applications in other QRNG schemes as well as RNG. For instance, the dedicated FPGA/GPU/CPU boards and algorithms developed could be used for fast QRNG based on high-resolution image sensors. Also, these methods may find application in quantum key distribution, in particular in key distillation procedures.

On the economical level, random number generation already today represents a relatively large market. Indeed, applications are not limited to field of cryptography, but include also gambling and lottery, Monte-Carlo simulation and others. The share or QRNG in this market will certainly increase in the future, as they offer stronger security compared to other physical RNG schemes. An important issue for QRNG will be to increase the rate while reducing the cost in order to remain competitive. The present project exactly addresses this issue.

On a societal level, the importance of high-quality random numbers increases rapidly, as the needs of privacy and security in a connected world increase. Indeed, internet banking and commerce, internet voting, virtual currencies and many other activities which require data security ultimately rely on randomness. In this context, the envisaged development of commercial self-testing QRNG could have strong impact.

2.5 Project plan

2.5.1 Methods & Milestones

The project's main goal is the development of a demonstrator for a self-testing QRNG. The latter should combine compactness, ease of implementation, low cost, and high randomness generation rate. The project features 3 main research lines and is thus naturally structured into three work packages (WPs). All three WPs are strongly interconnected and will benefit from the expertise of all partners.

WP1. Security analysis

The general aim is to provide an improved theoretical analysis of the self-testing protocol. In parallel, the procedure of randomness extraction will be investigated in detail, taking into account limitations of available technology. Finally, the potential of the self-testing approach will be more broadly explored.

Task 1.1: Trade-off between security and performance. The goal of this task is to determine the optimal trade-off between security and performance (i.e. randomness generation rate) for the self-testing QRNG protocol. A first direction consists in improving the current security proof. The latter is based on the assumption that the two states prepared by the source (preparation device) have an overlap that is lower-bounded by a given value, and this bound should hold true in any round of the experiment (see Fig. 1). For observed measurement data, this allows then to lower bound the min-entropy, which is a measure of the randomness contained in the raw data. Specifically, our aim here is to determine whether the rate can be enhanced by improving the theoretical analysis. Moreover, we will also investigate whether the assumption of "minimum overlap" can be partially relaxed. For

instance, it might be enough to ask that the assumption holds true only for a certain fraction of experimental rounds. If this is possible, then we will determine the minimal fraction of runs for which the assumption should hold. This will make the protocol more robust to technical imperfections, in particular to laser intensity fluctuations. A second direction consists in developing novel self-testing protocols. In particular, a natural extension of the present protocol consists in using more than two prepared states, which may lead to higher rates. We will characterize the performance of such multi-state protocols, and determine whether they are relevant from an experimental viewpoint or not.

Task 1.2: Randomness extraction. The final step of the self-testing QRNG protocol is the randomness extraction procedure (step 3 in Fig. 1). Based on a lower bound on the entropy of the raw data (estimated from the security analysis, step 2), the aim of the randomness extraction procedure is to extract the final random output bit string from the raw data, which is usually not perfectly random (only a minimal bound on the entropy is guaranteed). Randomness extraction is thus a purely classical procedure. In our proof-of-principle experiment we implemented randomness extraction based on Toeplitz hash functions. Implementing such a procedure at high speed (and if possible in real-time) represents a significant challenge for our demonstrator. It is therefore crucial to characterize the best adapted randomness extraction procedure, given available computational resources. We will thus thoroughly characterize performance and limitations of available processing devices, and identify the most suitable randomness extraction protocol.

Task 1.3: Further self-testing applications. The self-testing (or semi-DI) approach represents a promising solution, intermediate between the standard device-dependent approach and the fully device-independent one. Specifically, the self-testing approach combines the ease-of-implementation of the former with the strong security of the latter. While our work so far demonstrates the experimental relevance of the self-testing approach for randomness generation, here we will explore its potential for other quantum information processing tasks. In particular, we will develop self-testing quantum key distribution protocols, and determine their experimental feasibility. A starting point would be to consider prepare-and-measure QKD protocols using few (2-4) non-orthogonal states. Similarly, to our self-testing QRNG, the assumption would be a lower bound on the overlap between these states. The feasibility of implementations based on weak coherent states of light would then be investigated.

Deliverables

- Improved protocol for self-testing QRNG.
- Efficient randomness extraction on an embedded processing device.
- New cryptography protocol based on self-testing approach

WP2. Conception of the demonstrator

The goal of this WP is to define and characterize the different elements of the demonstrator, based on available electrical and optical components. We will use development kits for the embedded control and processing systems.

Task 2.1: Identify problems and limits with the current optical setup. Theoretically, it is difficult to take into account the behaviour of all elements of an experiment. This part will be dedicated to test the method to find the imponderables introduced by the experimental implementation. This part will be made in parallel with the Task 1.1 to find the simplest and the most robust approach. So during the stage, we will use the existing proof of principle experiments which offers the advantage to be flexible to test how the generated entropy is affected by the imperfections of the different elements. Moreover, the experimental setup will be updated to test the novel proposed approaches. The information collected during this phase we will help us to choose the dedicated optical components to implement the demonstrator.

Task 2.2: Specifications for optical components & signal processing**.** The target characteristics of the demonstrator will require specific optical elements. In the proof of principle, the bit rate was mainly limited by the dead-time of the detector. We will to explore different approaches to avoid this issue, like developing a fast passive quenching / active reset circuit to optimise the recovery time of standard silicon avalanche photodiode, or test other type of single photon detectors as Silicon photomultipliers, Discrete Amplification Photon Detectors. These two detector technologies allow to divide the photosensitive area in small cells. Each cell acts as a single-photon detector. So, with a large number of cells the probability of two consecutive detections in the same detector decreases. As a consequence, the global dead-time is reduced and the timing jitter of the detections becomes the limiting factor. This part is dedicated to find the best approach for the detection scheme. When this will be defined, we will choose the appropriate source which is compatible with the detector. Moreover, the electronic signals of these optical components need to be adapted to the FPGA input and output signals.

Task 2.3: Specifications for data post-processing. The aim of this task is to validate the implementation of the randomness extraction method with the available technologies, such as FPGA SoC, GPU or CPU or a mix of different technologies. The main challenge is to achieve the necessary computing power in order to output the random bits in real time with low energy consumption. Indeed, GPUs have a very high computing power, but their ratio performance vs. consumption is bad. At the opposite, this ratio is very good for FPGAs [Bert16, FBCS12]. We will investigate solutions and designs of FPGA in order to reduce the consumption. However, our system may also include a CPUs or GPUs, but it should be as small as possible to execute only processes that cannot be efficiently implement in FPGA. This means that, the control of the optical components, and the entropy estimation and extraction algorithms, will be realized with the most appropriate technologies. Note that, for example, the new Intel Stratix 10 SoC

FPGA include a Quad 64-bits ARM A53 and NVidia propose its Jetson TX1 module offering Quad 64-bits ARM A57 accompanied by a Maxwell 256 CUDA cores. The firmware will be implemented. Cutting algorithms into several parts involves appropriate software tools. Nowadays, High Level Synthesis (HLS) tools (from Xilinx, Intel, Nvidia ,...) allow to achieve hardware partitioning using different type of languages such as C / C ++, OpenCL, CUDA, VHDL used as input files.

Deliverables

- Fast single photon detector
- Firmware for the data post-processing system implemented in development kits

WP3. Realisation and test of the demonstrator

In this WP, we integrate the optics, the control and data post-processing units and test the demonstrator's performance.

Task 3.1: Integration of optics**.** To make the demonstrator as compact as possible, we plan to develop a dedicated board that include all the optical elements, i.e. the state preparation and the detection scheme with all the signal adaptation to make them compatible with the control and processing board. We need to take into account all the problems related to the integration as for example the optical or electrical parasite signals or the heat dissipation. Moreover, the optical elements include not only the laser and the detector but also linear optical elements necessary to shape the signal.

Task 3.2: Development of the embedded control and processing system**.** In this task, the dedicated electronics board needed to control the demonstrator and to process the data will be realized. This involves the following steps:

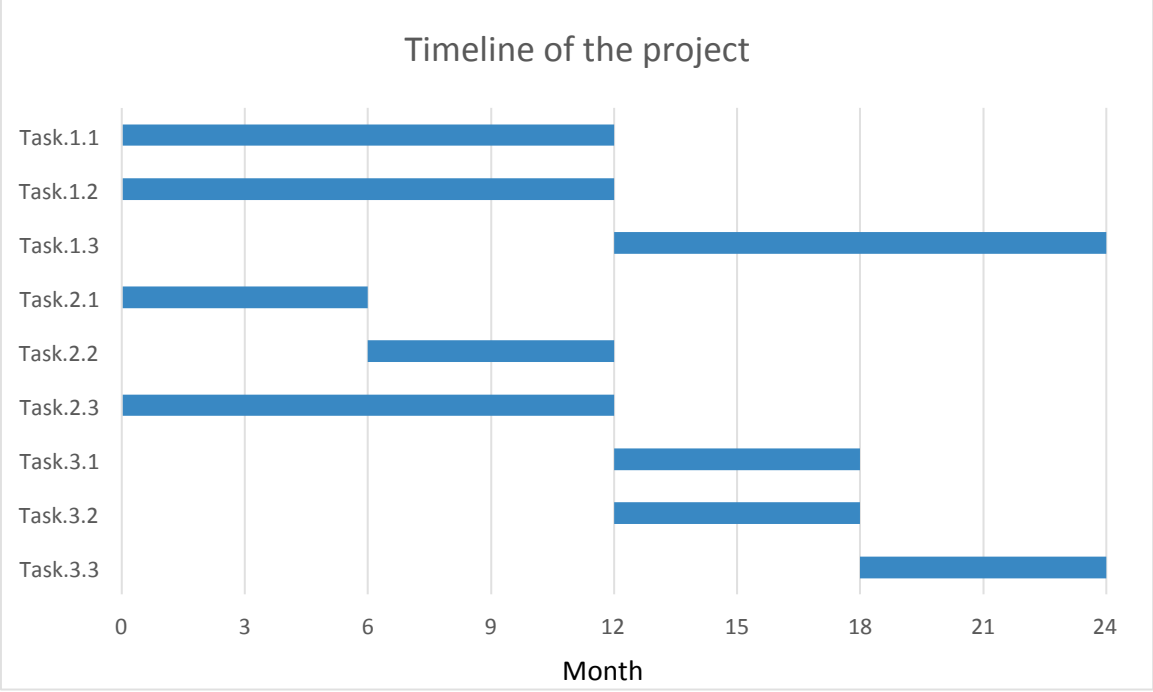
- Final components specification
  - Size and type of the FPGA/GPU and/or CPU; suitable power supplies, memory (DDR3/4), high-speed Communication Interfaces and etc.
- Design the schematics
  - Merge schematics from all part of the system, as optical electronics, schematic from development kit and etc. Moreover add all the requested companion chips for the embedded control and processing system
- Design the PCB, where the challenge will be:
  - Low noise power supply, low jitter clocking tree
  - High-speed DDR3/4 memory interface (size >16 Gbytes, rate > 4 Gbits/sec)
  - High-speed interface (> 6 Gbits/sec) to output raw datas, such as PCIe, USB 3.0, Ethernet 10G, SFP+, ...
- Manufacturing of the embedded system (PCB fabrication, mounting, ...)
- Adaptation of the created firmware, under WP1 & 2, to the produced embedded system (simulation and testing)
- Develop a Board Support Package (BSP) allowing to integrate a Linux (Operating System). This latter will natively support standard communication interface whereas

proprietary ones will require to develop our own drivers (the optical board for example).

Task 3.3: Test of demonstrator. To conclude the project, we plan to make an extensive characterisation of the demonstrator. First of all we need to develop a computer software to control the embedded system and to acquire the random bit string. To check if the optical part and the processing part work properly we need to have access to the raw data generated and the estimated entropy to make the verification on a computer. The main objective of this part is to prove that the QRNG is robust over a long time. We will study the amount of generated bits as a function of a set of parameters, like the working temperature or the instability of the power supply to define the working range of the device. All this information is mandatory for the realisation of a commercial device.

Deliverables

- A dedicated embedded control and processing system for the randomness extraction or the privacy amplification
- A computer software for the test of the demonstrator
- A self-testing QRNG demonstrator



Organisation of the project, benefit of the collaboration

The three project partners have very complementary expertise, all of which is needed for successful realisation of the project. Indeed the project requires a deep understanding of theoretical quantum information (Brunner group), experimental expertise in quantum optics

and photonics (Zbinden group), and strong know-how on design and exploitation of electronics board and hardware data processing (Messerli group). Arguably this span of fields is too large to be covered by a single research team and there is thus a clear benefit of the collaboration. Despite the variety of different research areas covered, the involved groups have shown very successful collaborations in the past. Specifically, the Zbinden and Messerli groups collaborated within the nano-tera project QCRYPT and more recently the Interreg project Easy-Phi. The Brunner and Zbinden groups had numerous collaborations, which lead to several publications in high-level peer-reviewed journals [LBLL15, BMEH17, GMM16].

The overall organisation of the project is expected to be straightforward. The roles of the different partners are well defined. The group have already demonstrated successful collaborations, and their physical proximity will facilitate regular interactions. Bi-weekly meetings between the groups in Geneva and monthly meetings between Yverdon and Geneva are planned, in addition to more frequent exchanges by email and phone.

Budget breakdown
All amounts in Swiss francs (CHF) [person month]

	Brunner	Messerli	Zbinden	Total
WP1	150628 [22pm]	34812 [4pm]	12800 [2pm]	198240 [28pm]
WP2	0	95733 [11pm]	66200 [15pm]	161933 [26pm]
WP3	13694 [2pm]	156655 [18pm]	80500 [17pm]	250849 [37pm]
Consumable		5000	38000	43000
Social security	37793	57440	36800	132033
Equipment				
Travel	8000	1500	3000	12500
Total	210115	351140	237300	798555

2.5.2 Innovation roadmap

The innovation roadmap is straightforward. We have demonstrated the feasibility of the protocol and submitted a patent application. The goal of this project is to make a compact and reasonably priced demonstrator in order to determine the commercial potential of self-testing QRNG. With the demonstrator and its specifications at hand, we can approach companies interested in commercialization. Preliminary interactions with the SME ID Quantique (Carouge, GE) are very encouraging. If their interest is confirmed, a prototype could be developed, possibly with the support of the CTI.

2.5.3 Risk management

Since the feasibility of the protocol has already been demonstrated in our proof-of-principle experiment [BMEH17], the overall risk of the project is arguably low. The thorough analysis performed during WP1 and WP2 will allow us to realize a fully functional demonstrator during WP3 with minimal risk.

The challenge is to find a commercially attractive trade-off between performance, complexity, and cost for the demonstrator. For all required components, both optics and electronics, a wide variety of products is available on the market. This provides flexibility for achieving such a trade-off. For example, there are many different options for implementing the single-photon detection platform. These include multiple cheap single-pixel detectors, more elaborate detectors like SiPM, or novel e-APDs. If economic need imposes it, even a standard single-pixel APD, like the one employed in our feasibility experiment, may be used. Moreover, concerning the cost of the electronics platform, we note that prices historically have decreased rapidly and this tendency continues. Hence, even if the components used for the demonstrator are relatively expensive, their price may become commercially competitive in the near future.

l'utilisation des Résultats Préexistants. Pour les éventuelles Résultats Préexistants matérialisés par des éléments intangibles, mais dont le Propriétaire souhaite qu'ils soient toutefois insérés dans l'annexe ad hoc du Projet, Le Propriétaire devra dûment en justifier le motif et celui-ci devra être recevable par les Partenaires.

3.2 Utilisation des résultats acquis ou obtenu dans le cadre de l'exécution du Projet

3.2.1 Utilisation des Résultats acquis ou obtenus dans la cadre de l'exécution du Projet par un seul Partenaire

Chaque Propriétaire reste propriétaire unique des Résultats acquis ou obtenus par lui-même dans le cadre du projet (ci-après les **« Résultats Propres**»).

Le Propriétaire accorde toutefois aux Bénéficiaires relativement aux Résultats Propres non couverts par un brevet :

- **une licence à des fins de réalisation du Projet**. Cette licence est limitée aux buts du Projet, gratuite, non-commerciale, non exclusive, non-transmissible, accordée uniquement si nécessaire au Projet, ne pouvant pas faire l'objet de sous-licences et strictement limitée à l'exécution et à la durée du Projet ;
- **aucune licence à des fins d'exploitation commerciale**. Toutefois, pour autant que les engagements déjà pris par le Propriétaire le permettent et sous réserve que le Propriétaire ne souhaite pas octroyer de licence exclusive, le Propriétaire s'engage à octroyer aux Bénéficiaires, sur demande de ce dernier et pour un prix favorable, une licence d'exploitation commerciale, non-exclusive, transmissible ou non transmissible selon les cas, pouvant faire l'objet de sous-licences ou pas selon les cas, d'une durée définie et dans le domaine d'activité du Projet ;
- **aucune licence à des fins de recherche et d'enseignement**.

Pour le cas où les Résultats Propres sont couverts par un brevet, chaque Bénéficiaire :

- reçoit du Propriétaire **une licence à des fins de réalisation du Projet**. Cette licence est limitée aux buts du Projet est gratuite, non-commerciale, non exclusive, non-transmissible, ne pouvant pas faire l'objet de sous-licences et strictement limitée à l'exécution et à la durée du Projet ;
- ne reçoit du Propriétaire **aucune licence à des fins d'exploitation commerciales**. Toutefois, pour autant que les engagements déjà pris par le Propriétaire le permettent et sous réserve que le Propriétaire ne souhaite pas octroyer de licence exclusive, le Propriétaire s'engage à octroyer aux Bénéficiaires, sur demande de ce dernier et pour un prix favorable, une licence d'exploitation commerciale, non-exclusive, transmissible ou non transmissible selon les cas, pouvant faire l'objet de sous-licences ou pas selon les cas, d'une durée définie et dans le domaine d'activité du Projet ;
- **est libre de les utiliser à des fins de recherche et d'enseignement** conformément à l'art. 9 LBI, al. 1b et 1d.

Pour chaque licence accordée relativement aux Résultats Propres, le Propriétaire confirme que ses Résultats Propres ont été développés ou acquis par lui-même, en toute indépendance et avec le soin requis et que, à sa meilleure connaissance, mais sans toutefois pouvoir le garantir, ces Résultats Propres n'enfreignent pas une propriété intellectuelle de tiers et sont à l'état de prototype de recherche. Pour le cas où la responsabilité civile et/ou pénale des autres Copropriétaires devait néanmoins être recherchée, le Copropriétaire ayant accordé la licence serait alors tenu de dédommager les autres Copropriétaires des éventuels préjudices subis.

Lorsque les Résultats Propres se matérialisent par un logiciel qui utilise une propriété intellectuelle de tiers, à savoir notamment :

- les logiciels Open Source selon licence GNU GPL / GNU LGPL, …, et/ou
- les logiciels propriétaires (shareware, …) dont la licence est téléchargeable sur le web et doit impérativement être approuvée avant toute utilisation,
- les logiciels propriétaires dont une licence doit impérativement être acquise à titre onéreux auprès du propriétaire dudit logiciel,

chaque Bénéficiaire devra alors acquérir, à titre gracieux ou onéreux, les licences ad hoc et respecter les conditions de licence du tiers propriétaire.

Sans l'accord préalable écrit du Propriétaire, les Bénéficiaires doivent traiter les Résultats Propres du Propriétaire de manière strictement confidentielle (cf. Règles, art. 5 - Confidentialité).

3.2.2 Utilisation des Résultats acquis et obtenus dans le cadre de l'exécution du Projet conjointement par des Partenaires et non couverts par un brevet ou une demande de brevet

En cas de Résultats acquis ou développés conjointement par les Partenaires dans le cadre du Projet et non couverts par un brevet ou une demande de brevet (ci-après les « **Résultats Conjoints** »), les Partenaires chercheront à identifier et à scinder la propriété intellectuelle des Résultats Conjoints en fonction des travaux effectivement réalisés par chaque Partenaire.

Si la scission peut être réalisée, la propriété intellectuelle des Résultats Conjoints attribuée à chaque Partenaire sera alors traitée comme des Résultats Propres (cf. 3.2.1).

Si la scission ne peut être réalisée, chaque Partenaire sera alors copropriétaire des Résultats Conjoints (ci-après le « **Copropriétaire** ») au prorata des investissements qu'il a consenti. Pour éviter tout doute, les investissements consentis seront déterminés selon le report financier final du Projet (rapport approuvé par la HES-SO).

Chaque Copropriétaire :

- **à des fins de réalisation du Projet**, est libre d'utiliser gratuitement les Résultats Conjoints non couverts par un brevet ou une demande de brevet ;
- **à des fins d'exploitation commerciale**, dès la date de fin officielle du Projet reconnue par la HES-SO, est libre d'exploiter gratuitement les Résultats Conjoints non couverts par un brevet ou une demande de brevet ainsi que d'accorder des licences commerciales à des tiers. Toutefois, ces licences seront non-exclusives et sous l'unique et entière responsabilité du Copropriétaire accordant la licence, sachant que la responsabilité des autres Copropriétaires ne peut en aucun cas être engagée ;
- **à des fins de recherche et d'enseignement**, est libre d'utiliser les Résultats Conjoints non couverts par un brevet ou une demande de brevet.

Chaque Partenaire qui n'est pas Copropriétaire reçoit des Copropriétaires :

- **une licence à des fins de réalisation du Projet**. Cette licence est limitée aux buts du Projet, gratuite, non-commerciale, non exclusive, non-transmissible, accordée uniquement si nécessaire au Projet, ne pouvant pas faire l'objet de sous-licences et strictement limitée à l'exécution et à la durée du Projet ;
- **aucune licence à des fins d'exploitation commerciale**. Toutefois, pour autant que les engagements déjà pris par le Propriétaire le permettent et sous réserve que le Propriétaire ne souhaite pas octroyer de licence exclusive, le Propriétaire s'engage à octroyer aux Bénéficiaires, sur demande de ce dernier et pour un prix favorable, une licence d'exploitation commerciale, non-exclusive, transmissible ou non transmissible selon les cas, pouvant faire l'objet de sous-licences ou pas selon les cas, d'une durée définie et dans le domaine d'activité du Projet ;
- **aucune licence à des fins de recherche et d'enseignement**.

Pour chaque licence accordée relativement aux Résultats Conjoints non couverts par un brevet ou une demande de brevet, chaque Copropriétaire confirme que ces Résultats ont été développés ou acquis par lui-même avec le soin requis et que, à sa meilleure connaissance, mais sans toutefois pouvoir le garantir, ces Résultats n'enfreignent pas une propriété intellectuelle de tiers et sont à l'état de prototype de recherche. Pour le cas où la responsabilité civile et/ou pénale du Propriétaires devait néanmoins être engagée, le Bénéficiaire ayant accordé la licence serait alors tenu de dédommager le Propriétaire des éventuels préjudices subis.

Lorsque les Résultats Conjoints se matérialisent par un logiciel qui utilise une propriété intellectuelle de tiers, à savoir notamment :

- les logiciels Open Source selon licence GNU GPL / GNU LGPL, …, et/ou
- les logiciels propriétaires (shareware, …) dont la licence est téléchargeable sur le web et doit impérativement être approuvée avant toute utilisation,
- les logiciels propriétaires dont une licence doit impérativement être acquise à titre onéreux auprès du propriétaire dudit logiciel,

chaque Copropriétaire devra alors acquérir, à titre gracieux ou onéreux, les licences ad hoc et respecter les conditions de licence du tiers propriétaire.

A moins d'un accord préalable écrit entre les Copropriétaires, chaque Copropriétaire n'est pas autorisé, durant le Projet, à accorder des licences à des tiers sur les Résultats Conjoints. Chaque Copropriétaire s'engage en outre à traiter de manière strictement confidentielle les Résultats Conjoints ou alors de les communiquer à des tiers sur la base d'un accord de confidentialité reprenant des exigences similaires aux Règles, art. 5 - Confidentialité.

Chaque Copropriétaire ne participe pas aux éventuelles retombées économiques réalisées par les autres Copropriétaires liés aux Résultats Conjoints.

3.2.3 Utilisation des Résultats Conjoints acquis et obtenus dans le cadre de l'exécution du Projet et pouvant donner lieu à un brevet

Lorsque les Résultats Conjoints peuvent donner lieu à un brevet (ci-après les « **Résultats Conjoints Brevetables/Brevetés** »), les Copropriétaires s'entendront sur l'opportunité d'un dépôt de brevet.

Les Copropriétaires s'engagent en outre à respecter la confidentialité liée aux Résultats Conjoints Brevetables/Brevetés (cf. Règles, art. 5 - Confidentialité) et s'abstiendront de toute publication avant la date de dépôt de la demande de brevet, à moins que les Copropriétaires s'accordent sur une publication qui ne compromette pas l'obtention d'un brevet.

Si les Copropriétaires décident de ne pas soumettre une demande de brevet ou que le brevet ne peut être délivré ou que celui-ci tombe dans le domaine public, les Copropriétaires s'accordent alors à gérer les Résultats Conjoints pouvant donner lieu à un brevet ou une demande de brevet conformément à l'art. 3.2.2 (des Résultats acquis et obtenus dans le cadre de l'exécution du Projet conjointement par des Partenaires et non couverts par un brevet ou une demande de brevet)

Si les Copropriétaires décident de soumettre une demande de brevet, ceux-ci s'engagent à n'octroyer aucune licence relative aux Résultats Conjoints Brevetables/Brevetés durant l'exécution du Projet. Dans des cas exceptionnels et justifiés, les Copropriétaires peuvent à l'unanimité de ceux-ci en convenir différemment.

Si un ou plusieurs Copropriétaires souhaite(nt) déposer une demande de brevet (ci-après les « **Déposants** ») relative aux Résultats Conjoints Brevetables/Brevetés, alors qu'un ou plusieurs autres Copropriétaires ne le souhaite(nt) pas (ci-après les « **Abstinents** »), les Déposants seront alors libres de déposer une demande de brevet en leurs noms. Les Abstinents devront dans tous les cas être mentionnés comme co-inventeur.

Pendant la période de dépôt d'une demande de brevet et, ce, jusqu'à la publication de cette dernière, les Abstinents s'engagent à traiter les informations liées à la demande de brevet de manière strictement confidentielle.

Une fois la demande de brevet publiée, les Abstinents se voient octroyer par les Déposants relativement aux Résultats Conjoints Brevetables/Brevetés :

- **une licence à des fins de réalisation du Projet**. Cette licence est limitée aux buts du Projet, gratuite, non-commerciale, non exclusive, non-transmissible, ne pouvant pas faire l'objet de sous-licences et strictement limitée à l'exécution et à la durée du Projet ;
- **aucune licence à des fins d'exploitation commerciale** ;
- **une licence à des fins de recherche et d'enseignement sur la demande de brevet puis, si brevet, libre de les utiliser gratuitement**.

Pour chaque licence accordée relativement aux Résultats Conjoints Brevetables/Brevetés, Chaque Copropriétaire confirme que ses Résultats Conjoints Brevetables/Brevetés ont été développés ou acquis par lui-même, en toute indépendance et avec le soin requis et que, à sa meilleure connaissance, mais sans toutefois pouvoir le garantir, ces Résultats Conjoints Brevetables/Brevetés n'enfreignent pas une propriété intellectuelle de tiers et sont à l'état de prototype de recherche. Pour le cas où la responsabilité civile et/ou pénale des autres Copropriétaires devait néanmoins être engagée, le Copropriétaire ayant accordé la licence serait alors tenu de dédommager les autres Copropriétaires des éventuels préjudices subis.

Lorsque les Résultats Conjoints Brevetables/Brevetés se matérialisent par un logiciel qui utilise une propriété intellectuelle de tiers, à savoir notamment :

- les logiciels Open Source selon licence GNU GPL / GNU LGPL, …, et/ou
- les logiciels propriétaires (shareware, …) dont la licence est téléchargeable sur le web et doit impérativement être approuvée avant toute utilisation,
- les logiciels propriétaires dont une licence doit impérativement être acquise à titre onéreux auprès du propriétaire dudit logiciel,

chaque Copropriétaire devra alors acquérir, à titre gracieux ou onéreux, les licences ad hoc et respecter les conditions de licence du tiers propriétaire.

Les Abstinents ne participent pas aux retombées économiques liées aux Résultats Conjoints Brevetables/Brevetés.

Pour le cas où un Déposant ne souhaiterait plus maintenir la demande de brevet, respectivement le brevet, celui-ci passerait alors du statut de Déposant à celui d'Abstinent à partir de la date où sa contribution financière au maintien de la demande de brevet, respectivement du brevet, est échue.

Les Déposants s'entendront sur la meilleure manière de valoriser les Résultats Conjoints Brevetables/Brevetés. A défaut d'entente entre les Copropriétaires et après une dernière réunion qui actera que le différend n'a pas pu être résolu selon l'art. 7 (Différends, droit applicable et for) des Règles, chaque Déposant sera alors :

- **à des fins de réalisation du Projet**, est libre d'utiliser gratuitement les Résultats Conjoints Brevetables/Brevetés ;
- **à des fins d'exploitation commerciale**, est libre, dès la date de fin officielle du Projet reconnue par la HES-SO, d'exploiter commercialement les Résultats Conjoints Brevetables/Brevetés, et d'accorder des licences commerciales à des tiers. Toutefois, ces licences seront non-exclusives uniquement et sous l'unique et entière responsabilité du Déposant accordant la licence, sachant que la responsabilité des autres Déposants ne peut en aucun cas être engagée;
- **à des fins de recherche et d'enseignement**, est libre d'utiliser les Résultats Conjoints Brevetables/Brevetés.

Pour chaque licence accordée relativement aux Résultats Conjoints Brevetables/Brevetés, Chaque Copropriétaire confirme que ses Résultats Conjoints Brevetables/Brevetés ont été développés ou acquis par lui-même, en toute indépendance et avec le soin requis et que, à sa meilleure connaissance, mais sans toutefois pouvoir le garantir, ces Résultats Conjoints Brevetables/Brevetés n'enfreignent pas une propriété intellectuelle de tiers et sont à l'état de prototype de recherche. Pour le cas où la responsabilité civile et/ou pénale des autres Copropriétaires devait néanmoins être engagée, le Copropriétaire ayant accordé la licence serait alors tenu de dédommager les autres Copropriétaires des éventuels préjudices subis.

Lorsque les Résultats Conjoints Brevetables/Brevetés se matérialisent par un logiciel qui utilise une propriété intellectuelle de tiers, à savoir notamment :

- les logiciels Open Source selon licence GNU GPL / GNU LGPL, …, et/ou
- les logiciels propriétaires (shareware, …) dont la licence est téléchargeable sur le web et doit impérativement être approuvée avant toute utilisation,
- les logiciels propriétaires dont une licence doit impérativement être acquise à titre onéreux auprès du propriétaire dudit logiciel,

chaque Déposant devra alors acquérir, à titre gracieux ou onéreux, les licences ad hoc et respecter les conditions de licence du tiers propriétaire.

A moins d'un accord préalable écrit entre les Déposants, chaque Déposant n'est pas autorisé, durant le Projet, à accorder des licences à des tiers sur les Résultats Conjoints Brevetables/Brevetés. Chaque Copropriétaire s'engage en outre à traiter de manière strictement confidentielle les Résultats Conjoints Brevetables/Brevetés, pour le moins, tant que les demandes de brevet ne sont pas publiées ou, alors, de communiquer à des tiers ces résultats sur la base d'un accord de confidentialité reprenant des exigences similaires aux Règles, art. 5 - Confidentialité.

Les Déposants devront impérativement s'accorder à l'unanimité en cas de vente des Résultats Conjoints Brevetables/Brevetés à un tiers.

Pour autant que les Déposants participent aux frais d'administration et de maintien Résultats Conjoints Brevetables/Brevetés, les retombées économiques liées des Résultats Conjoints Brevetables/Brevetés, c'est-à-dire les bénéfices résiduels réalisés par chaque Déposant, seront réparties entre les Déposants supportant les frais susmentionnés au prorata des investissements consentis par chaque Déposant. Pour éviter tout doute, les investissements consentis seront déterminés selon le report financier final du Projet (rapport approuvé par la HES-SO).

Sitôt qu'un Déposant cesse de payer sa quotepart aux frais d'administration et de maintien de la demande de brevet, respectivement du brevet, il perd son droit aux retombées économiques liées aux Résultats Conjoints Brevetables/Breveté, respectivement d'un brevet.

Les Déposants s'entendront et désigneront un Déposant qui s'occupera de toute l'administration liée au dépôt de brevet et au maintien de celui-ci.

Chaque Déposant est tenu d'assumer, au prorata de l'investissement qu'il a consenti tous les frais liés au dépôt de brevet et au maintien de celui-ci.

3.3 Utilisation des Résultats nécessaires à une start-up issue d'une école de la HES-SO

Si une start-up est créée au sein d'une école de la HES-SO afin de valoriser les Résultats du Projet, les Propriétaires/Copropriétaires, cas échéant les Déposants, des Résultats nécessaires à cette valorisation (Résultats Préexistants, Résultats Propres, Résultats Conjoints, Résultats Conjoints Brevetables/Brevetés) s'engagent à négocier avec la Start- up des conditions favorables et motivantes de transfert et/ou d'utilisation desdits Résultats. Seuls les Propriétaires/Copropriétaires, cas échéant les Déposants, auront le pouvoir de négocier avec la start-up.