Practical aspects of security certification for commercial quantum technologies

Nino Walenta[a], Mathilde Soucarros[b], Damien Stucki[b], Dario Caselunghe[b], Mathias Domergue[b], Michael Hagerman[a], Randall Hart[a], Don Hayford[a], Raphaël Houlmann[b], Matthieu Legré[b], Todd McCandlish[a], Jean-Benoît Page[b], Maurice Tourville[a], Richard Wolterman[a]

[a]Battelle Memorial Institute, 505 King Avenue, 43201 Columbus (OH), United States;
[b]ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge/Geneva, Switzerland

ABSTRACT

Quantum random number generation (QRNG) and quantum key distribution (QKD) are the first applications of quantum physics at the level of individual quanta that have matured into commercial products. Both have been commercially available for over 10 years and increasingly adopted in information security systems. Current efforts focus on standardization and certification of QRNG and QKD devices and their components in order to validate the technology and enable more widespread adoption. Since no official certification scheme specific to quantum devices has been devised so far, alternative options must be investigated. This paper describes our approaches and efforts to enable compliance of commercial QRNG and QKD network devices with security standards such as AIS 20/31[1] and FIPS 140-2.[2]

Keywords: Network security, Quantum random number generator, Quantum key distribution, Certification, Standardization

1. INTRODUCTION

Quantum random number generation (QRNG) and quantum key distribution (QKD) are the first applications of quantum physics at the level of individual quanta that have matured into commercial products. Both have been commercially available for over 10 years and increasingly adopted in information security systems. Current efforts focus on standardization and certification of QRNG and QKD devices and their components in order to validate the technology and enable more widespread adoption.[3]

As with any other complex system, the practical application of quantum devices requires that an implementation is fully trusted by its users, even without complete knowledge about every detail of the underlying technology. In the realms of information security systems this implies that the owner of an ICT (information and communications technology) device is assured that the implemented security measures are sufficient to counter any possible attack, and that they are implemented correctly. This assurance is what security certification can provide: it aims at establishing trust by certifying that a device has been designed, implemented and independently evaluated following a standardized methodology. Additionally, certification provides benefits for manufacturers in that it minimizes vulnerabilities and risks, and overall improves the product quality by enforcing consequent assessment of security functions during the design and development phase.

For conventional cryptographic modules several security certification standards exist, most prominently the "Common Criteria for IT security evaluation" (CC),[4] and the U.S. domestic "Federal Information Processing Standards" 140-2 (FIPS 140-2)[2] developed by NIST and recognized by several countries and industries. Both require that the device and its supporting documentation are examined by an accredited testing laboratory and reviewed by a government agency before the latter issues the certificate. Their main difference is that the FIPS 140-2 standard specifies a set of cryptographic security requirements related to the design and implementation of cryptographic modules via a strict specification of choices that have to be made, while Common Criteria

Corresponding authors:
N. Walenta: walenta@battelle.org
M. Soucarros: mathilde.soucarros@idquantique.com

actually specifies a methodology for writing standards and for evaluating against them. In direct comparison, Common Criteria takes a wider look at the overall system design and functionality, where nearly every aspect and process from inception, to development, commercial release, support, and overall use of a product is reviewed and scrutinized. Any organization or client can specify their requirements according to their needs in a CC protection profile, and a vendor can choose which protection profile to follow when pursuing a certification for a product.

However, since no official certification scheme specific to quantum devices has been devised so far, alternative options must be investigated. This paper describes our approaches and efforts to enable compliance of commercial QRNG and QKD network devices with security evaluations such as AIS 20/31[1] and FIPS 140-2.[2]

In the first part, we present the steps taken for a standalone commercial quantum random number generator (IDQ Quantis AIS31[5]) so that it complies with the BSI AIS 20/31 standard. This standard describes a methodology for the evaluation of random number generators (RNGs), where RNGs are grouped under different categories. Depending on the category, numbers are generated with a guaranteed minimum degree of randomness and are appropriate for different uses in cryptographic applications. For this purpose, parameters such as the entropy rate, uniformity and unpredictability of generated bitstreams are taken into consideration and must be measured through a meticulous evaluation of our generator as well as statistical tests.

Secondly, we present our approach for developing and certifying a QKD-Trusted Node (QKD-TN) network architecture and hardware, which enables QKD-based key distribution amongst multiple users over arbitrarily long distances. Importantly, it strives for the first time for compliance of QKD with the FIPS 140-2 Level 3 security standard for information systems in order to allow its use for example in governmental networks and agencies.

2. MAKING A QRNG COMPLIANT TO AIS 20/31

In this section, we present the approach taken for making a standalone commercial QRNG (IDQ Quantis AIS31[5]) comply with the BSI AIS 20/31 standard.[1] Though it is not part of a certification scheme, this standard is well recognized for its guidelines concerning RNG implementation. This AIS 20/31 standard describes a methodology for the evaluation of RNGs, where they are grouped into different categories. Under this classification, a QRNG falls under the category of physical true generators (PTG) that possess a physical source of entropy without restriction on the physical process involved. Within the PTG family, there are three classes of RNGs:

Class PTG.1 The generator must detect a failure of the entropy source and statistical defects on the internal random numbers (after post-processing). The generated numbers are not unpredictable, both in the past and in the future.

Class PTG.2 The generator must additionally comprise a stochastic model of the entropy source and statistical tests on the raw random numbers (before post-processing). The generated numbers may have a small entropy defect but should not be subject to guessable attacks.

Class PTG.3 The generator must additionally implement a cryptographic post-processing process. The generated numbers are guaranteed secure on one part by information-theoretical security and on the other part by computational security.

For the purpose of our product evaluation, we chose class PTG.3 that guarantees the highest degree of security on the generator's output. The processes involved in making our QRNG belong to this class as described in Figure 1. In practice, a cryptographic post-processing procedure, as well as health tests, were therefore added to the random number generation process. A rigorous mathematical model of the entropy source based on quantum phenomena was derived in order to explain the amount of entropy produced. The following sections explain the steps that led to the completion of the AIS 20/31 compliance evaluation.

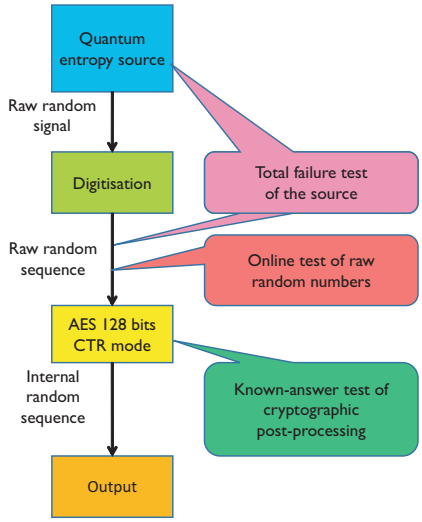


Figure 1. The AIS 20/31 version of the Quantis adds a cryptographic post-processing (AES 128 bits in CTR mode) as well as tests on the entropy source, the random numbers and the post-processing.

2.1 Security target

The security target is a document describing the device under evaluation and its working environment. Its goal is to specify which parts of the device must be examined (may they be electronics, mechanics or software) and the limits of its specifications (temperature resistance, tampering, etc.). In the case of the Quantis, we specify that the device should be installed inside a restricted and regulated room so that variations of temperature do not exceed the $0 - 40\,^{\circ}\mathrm{C}$ range and variations on the voltage supply do not exceed $5V \pm 10\%$.

2.2 Entropy

The AIS 20/31 standard requires demonstrating that the entropy produced by our device is sufficient. The two methods described here realize a theoretical and practical evaluation of the entropy of our device, for the raw and internal random numbers.

2.2.1 Stochastic model of the entropy source

As requested starting from PTG.2 classes, a stochastic model of the entropy source must be provided. This model allows verification that the physical processes involved are suitable for the generation of random numbers and that an entropy rate can be derived from it.

RNGs based on classical sources of entropy usually rely on imperfections in electronic components to extract randomness. For instance, typical designs involve transistors, ring oscillators (creating jitter) or resistors (thermal noise). The Quantis entropy source is based on quantum physics, following the basic principle explained in Figure 2. The randomness exploited in this design is provided by the wave-particle duality property of photons. Because of this property, a photon propagates like a wave and takes all possible paths but it is detected like a particle meaning that only one detector will see it. It is not possible to guess which detector will be activated so the process is random.

The Quantis entropy source is based on this principle with the following specifications. A LED illuminates two detectors D_A and D_B realized by Single Photon Avalanche Diodes (SPAD) during a certain period of time. If a detector clicked (detected a photon) during this time then we assign the value '1' to it otherwise it is a '0'. At time t, both detectors are then either in state (X_A for D_A and X_B for D_B) '0' or '1'. From the state of the detectors at time t we generate a bit thanks to a von Neumann-like process: if both X_A and X_B are equal to '0' or '1' then we discard the result, otherwise we take the value X_A.

In practice, electronic and optical components are not perfect and the following effects can be observed:

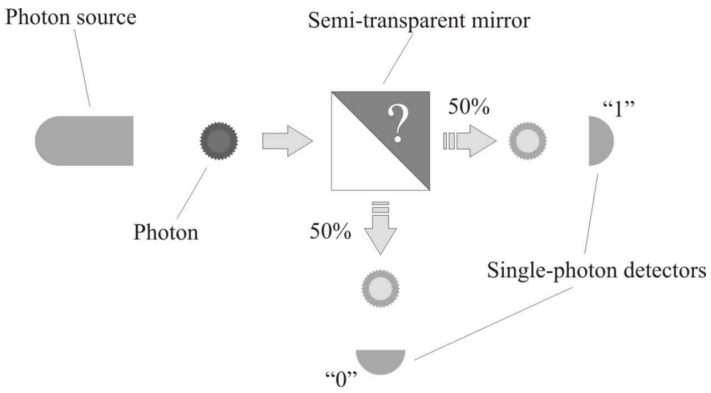


Figure 2. The principle of quantum bits generation can be illustrated as follows: photons are sent into a semi-transparent mirror and are either transmitted or reflected to two different detectors.

- Difference in the probabilities of detections between the two detectors. This is due to SPAD efficiencies which are not exactly the same.
- Darknoise: Detectors can click even if a photon was not emitted. This is due to noise around the component.
- Afterpulses: After a detection at time t it is more likely to have a detection at time $t+1$. This is due to electrons that stay trapped inside the component.
- Crosstalk: A detection on one detector can trigger a click on the other detector. This is due to electrical and optical coupling.

Taking those defects into consideration, it was possible to define the probability of having a state $X_t = (X_A, X_B)$ at time t. Because the state of the detectors is correlated in space (crosstalk) and in time (afterpulses), we ended up with a transition matrix giving us the probabilities $P(X_t|X_{t-1})$. From this matrix we could deduce the probabilities $P(Y_t|Y_{t-1})$ of having a '0' or a '1' in the bitstream after the von Neumann procedure. This gave use a final transition matrix from which we could compute the entropy of the bitstream.

After writing the stochastic model of the source, not only did it give us a result for the entropy of the system but we could also run simulations and see the way each parameter can influence this result. As required by the AIS 20/31 standard for the PTG.3 class, we verified that the source generates at least 7.976 bits/byte of entropy.

2.2.2 Offline tests

As a means of evaluating the entropy, we ran the different statistical tests described in the standard. They consist of two test procedures, A and B that respectively check that the internal random numbers cannot be distinguished from true random numbers and that the entropy of the raw random numbers is large enough. The procedures comprise different statistical tests estimating the amount of bias and correlation in the bitstreams.

2.3 Cryptographic post-processing

As required by the PTG.3 class specification, a cryptographic post-processing algorithm must be added. The goal of this processing is to ensure backward and forward secrecy (impossibility to retrieve previous and future outputs when knowing the current one) and enforce computational security. We chose to implement an AES 128 bits in CTR mode as recommended by the NIST.[6]

The raw random numbers (from the entropy source) are used as an entropy input to the algorithm and the internal random number (output) secrecy is guaranteed by the AES properties and the way it is used as defined for class PTG.3:

- The entropy input must contain at least 128 bits of entropy. The entropy source generates at least 7.976 bits/byte of entropy, which means that we chose an entropy input of length 17 bytes.

- The output data rate (AES output) must not be higher than the input data rate (entropy input). It means that each AES round produces 17 bytes of internal random numbers.

2.4 Online tests

The aim of the online test is to detect an error as soon as possible in the generation process. This helps keeping the system secure and stopping it as soon as possible when necessary. For class PTG.3 RNGs, three kinds of tests are required; we detail them in the following sections.

2.4.1 Total failure test of the source

This test verifies that the physical parameters of the entropy source stay in a normal range. In practice, we monitor the amount of afterpulses and crosstalk and verify that the outcome to a simple χ^2 test on the raw random numbers is not outside of some defined bounds. If this test fails, then the device is disabled as it means that it works incorrectly and the generated numbers are not secure anymore.

2.4.2 Online test of raw random numbers

This procedure is executed online and continuously on the raw random numbers. The goal is to detect defects in the statistics computed on the bitstream and warn the user of a problem. This procedure ideally comprises tests that detect typical defects encountered with the entropy source. For the Quantis, it means bias (due to different detector efficiencies) and correlations (due to afterpulses and crosstalk). We implemented a χ^2 test so that we could detect those defects. The χ^2 test compares distribution of raw bit patterns to an ideal distribution.

2.4.3 Know-answer test of cryptographic post-processing

The aim of this test is to verify the correct functioning of the cryptographic post-processing. In practice, it is realized by known-answer tests realized at regular intervals. The known-answer test consists of always inputting the same bitstreams into the AES algorithm and verifying that the output stays identical. It allows us to detect if there was tampering on the post-processing algorithm.

2.5 Evaluation process

The Quantis conformity assessment to the AIS 20/31 standard was performed by an independent evaluation facility (CEST-LETI, Grenoble, France). The evaluation consisted of reviewing all documents and information pertaining to the device and verifying they followed the standard requirements. They also conducted tests on the device in different conditions and verified the claimed security functionalities. At the end of the process, they confirmed compliance of our QRNG with the AIS 20/31 standard.

3. TRUSTED NODE QKD NETWORK

Quantum key distribution[7,8] (QKD) systems realize an essential cryptographic primitive, namely the secure distribution of cryptographic keys between remote parties. Cryptographic keys are of great importance in information and communications technology (ICT) systems, and their security is crucial to protect the confidentiality, integrity and authenticity of data transmitted over ICT networks. Today's algorithmic key distribution methods are based entirely on mathematical methods whose general acceptance relies on restrictive assumptions and beliefs about the capabilities of potential eavesdroppers, but no rigorous proof that their security is adequate. These methods are increasingly threatened by advancing technologies such as improving computational resources, new attack algorithms and, importantly, the emergence of quantum computers. Moreover, their security is not future-proof since the simple tactic of recording network data now and decoding later (store-and-decrypt attack) is likely to reveal information in the near future that appears secure today.

In contrast to algorithmic key distribution methods, QKD protects key transmissions directly on the physical communication layer by using quantum states of light to encode and exchange information between remote parties. From this shared quantum information, highly secure cryptographic keys are then derived, which can be safely used with conventional algorithms to encrypt or authenticate data. Any attempt to eavesdrop on a QKD key can be detected before it is used, in which case the key is rejected. The security of QKD arises from fundamental laws of quantum physics, and the principle has been proven information-theoretically secure against

arbitrarily powerful eavesdroppers, even in the presence of quantum computers. Thus, QKD is invulnerable to increasing computational power or quantum computers, and can promise future-proof protection against later code-breaking.

Despite these obvious benefits, and the availability of commercial products for over a decade, the commercial use of QKD has so far been restricted to some niche applications. One often cited reason why widespread adoption has been hindered is the limitation of the maximum QKD transmission distance. The nature of the physical quantum optical communication channel doesn't allow for optical amplification of the transmitted signals, limiting the maximum distances of the fiber or free-space links to a few hundred kilometers to date.[9,10] However, this limitation is outweighed by the very high key distribution rates, with modern QKD systems achieving ∼Mbps (megabits per second). Quantum repeaters promise to overcome the distance limitation of QKD, but while they are the subject of extensive active research, their commercial availability is not expected in the very near future.

3.1 Certification and standardization efforts related to QKD

A second important reason, on which we will focus here, is the lack of security certification standards for QKD.[11] Over the last years, several approaches have been taken in order to develop similar security certification standards for quantum key distribution.

The first started as a sub-project during the European "SECOQC" FP6 project,[12] and accomplished establishment of a CC protection profile for the security specification of the common digital part within a QKD network. However, the actual quantum physical key generation sub-system couldn't be included in this profile due to the lack of a methodology for assessing its practical security. This deficiency motivated the formation of the ETSI Industry Specification Group on QKD (ISG-QKD),[3,13] with members comprising telecom operators and industry, small and medium-sized enterprises, metrology institutes, government labs, and universities. Within the ISG-QKD, two parallel approaches were taken to establish a security specification for QKD. The first followed the FIPS 140-2 security specification for random number generators, where a QKD link was interpreted as a special form of a RNG that generates random keys simultaneously at two distinct locations. Although this approach even comprised the QKD protocol level, no certification of the physical key generation processes could be accomplished for similar reasons as before.

The second, parallel ISG-QKD approach for security certification for QKD, which is still ongoing, is called "pragmatic approach". It aims at a specification including the quantum optical sub-system by incorporating a standardized quantitative assessment of the discrepancies between a real system and its underlying theoretical security proof model through well-defined parameters and test procedures.[14] Although this "pragmatic approach" of the ISG-QKD initiative has made significant progress, especially due to the support of several metrology organizations, the process is still on-going and requires more research in order to complete the development of such standards. In conjunction, accredited evaluation labs would require purposive training and instruction in order to become familiar with QKD and the specific hacking and side channel attacks before they are able to perform evaluation against these standards.

3.2 QKD in the scope of the FIPS 140-2 certification standard

In order to drive the commercial deployment of QKD already today, especially in environments which strictly rely on certified products, alternative options for rendering QKD systems compliant with existing ICT security certification standards have to be pursued until the development of specific standards for the quantum-optical sub-system has been finalized. In the following, we present our approach for architecture and hardware of a QKD Trusted Node (QKD-TN) network which is compliant with the FIPS 140-2 security certification and evaluation standard. The QKD-TN conforms to the Advanced Telecommunications Computing Architecture (ATCA) requirements specification[15] and enables highly secure distribution of cryptographic keys based on QKD between multiple users and over arbitrarily long distances.

The FIPS 140-2 standard specifies 11 areas of cryptographic security requirements related to the design and implementation of a cryptographic module. The areas that shall be satisfied include 1) the specification of the cryptographic module; 2) the information flow and its segregation through ports and interfaces; 3) the supported operators roles, which services, operations and functions can be performed and how they are authenticated; 4) a finite state model of the high-level states and how transitions occur; 5) the physical security against tampering

and robustness against extreme environmental conditions; 6) the operating system that the module uses or is used by; 7) cryptographic key management including generation, entry, output, storage and destruction of keys; 8) electromagnetic interference and compatibility; 9) self-tests and consequences of their failure; 10) documentation which assures that the module is well designed and implemented; and 11) how other attacks are mitigated. During evaluation, each area gets rated by a level between 1-4, the highest and most stringent being FIPS 140-2 level 4. The overall rating is determined by the lowest in all eleven areas.

While most of the eleven areas do not interfere with an application to QKD per se, the most problematic requirements are related to the information flow through ports and interfaces, and the cryptographic key management. In contrast to Common Criteria, FIPS 140-2 defines a self-contained catalog of approved methods and cryptographic functions which can be used for generation, entry, output, storage and destruction of keys, but explicitly forbids the use of any unstated method or function. Amongst others, no critical security parameter or key shall ever leave the cryptographic module without encryption by an approved method. However, the fundamental quantum-physical principles which guarantee the security of keys distributed by QKD are not contained in the catalog of approved methods, and hence, from a FIPS point of view the QKD keys are distributed without any approved protection. Moreover, the information-theoretical secure QKD post-processing algorithms which are typically used for error correction, privacy amplification and authentication are, although provably secure, not approved.

At first glance this might indicate that certification of QKD in compliance with FIPS 140-2 is out of scope. Fortunately, it turns out that there are two hidden possibilities to achieve this compliance by just minor modification of the QKD post-processing. The first possibility is to use the secret and authenticated QKD key as additional input to an approved deterministic random number generator (DRNG) as shown in the left of Fig. 3. The main entropy input provided for the seed of this DRNG has to be generated by an approved method with a sufficient amount of entropy and must be kept secret. The seed input needs to be shared secretly by both, the QKD transmitter and receiver station, using an approved method based on manual key entry or key transportation during initialization. Besides this main entropy input, FIPS 140-2 (more specifically the referenced recommendation for random number generation[6]) allows for an additional entropy input which is provided during re-seeding or during request for pseudo-random bits. This additional input has relaxed requirements and doesn't need to be generated by an approved method, and therefore can be the secret and authenticated QKD key. Most important for our purposes, the final DRNG output key is then generated by an approved method which is compliant with FIPS 140-2, but based on the QKD key. While this method has the advantage that the rate of generated keys can be increased in comparison to the QKD key rate, the biggest disadvantage is that the information-theoretical security of the QKD key is lost due to the DRNG processing. This disadvantage can be circumvented using the method which we describe in the following.

The second possibility, shown in the right of Fig. 3, is based on a FIPS 140-2 approved method for generating symmetric keys by combining component symmetric keys with other data items that are independent of the component keys to form the final key.[16] The component symmetric keys have to be generated or established using any method that ensures their independence from the data items, and similar to the DRNG method needs to be shared secretly by the QKD transmitter and receiver station. While the key values are required to be secret, the data item values are not strictly required to be kept secret. In the context here, the data items will be the secret and authenticated QKD output. The component symmetric keys can be continuously generated using a DRNG, where as before the seed input needs to be shared secretly by both QKD stations, using an approved method based on manual key entry or key transportation during initialization. One approved method for combining the symmetric keys with the QKD output is bit-wise exclusive-oring (XORing) where the length of each component key and each QKD output item shall be equal to the length of the final key. In contrast to the previous method based on the DRNG, the XOR operation passes in a provable manner the information-theoretical security of the QKD key without any degradation on to the final output key, while at the same time enabling an approved method for key generation based on QKD that is compliant with FIPS 140-2.

Both described methods can easily be added as a final procedure to the standard QKD post-processing and are very fast, especially the XOR-based key generation method. Although the QKD key is an essential input to these methods, which significantly increases the security of the final output key, no evaluation and testing of the actual quantum channel and its related components is strictly required, thus eliminating the need for

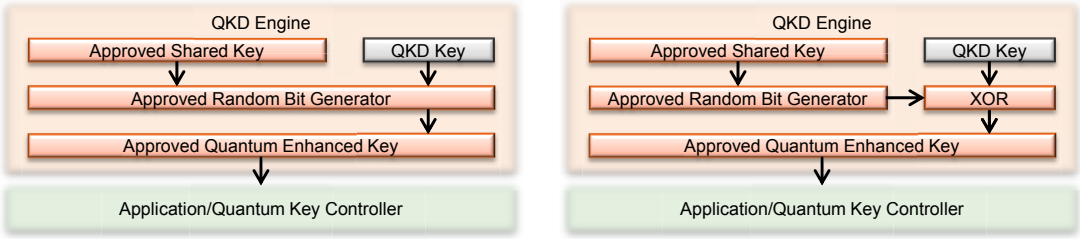


Figure 3. Illustration of two methods for generating quantum keys in compliance with the FIPS 140-2 certification standard.

special training of the evaluation labs about quantum hacking. Moreover, the security of the final output key is as strong as the strongest of the two input components. Thus, under normal circumstances the security of the produced output is as strong as the security of QKD, but even in case of a failure of the QKD system the whole key generation process is not compromised below the level of conventional cryptographic key generation methods.

3.3 Development of a Trusted node QKD network in compliance with FIPS 140-2

In a collaborative effort between Battelle and ID Quantique we have been developing architecture and hardware for a scalable multi-user quantum key distribution network that enables highly secure distribution of cryptographic keys based on QKD between multiple users and over arbitrarily long distances.[17] Conceptually, the QKD-TN network architecture is a special incarnation of the Trusted Node (or Trusted Repeater) paradigm, similar to all QKD networks demonstrated to date.[12,18–23] On the physical layer, trusted relay networks establish point-to-point QKD links pairwise between neighboring network nodes, which form the quantum back bone, and continuously generate pairs of highly secure shared symmetric keys. Via a chain of intermediate trusted nodes, secure keys can be shared not only between neighboring nodes, but also between nodes that are not directly connected to each other by a quantum link. However, in contrast to traditional approaches we have implemented additional measures in order to reduce the trust requirements in intermediate nodes and increase the security against threats imposed by insider attacks as shown in Fig. 4 and explained below.

At any network node the generation of a cryptographic user key and its distribution to the desired target node can be initiated. Upon request, a user key is generated at the initiating node using an approved DRNG with the entropy seed derived from the certified QRNG described in section 2. The initiating node then initiates a FIPS 140-2 approved key transport scheme with the target node by requesting the target node to generate an RSA-based public-private key pair and to publish the public key. Upon validation of its authenticity, the initiating node uses the target node's public key to encrypt the user key. This key transport scheme not only serves as the basis for distributing the user keys in compliance with FIPS 140-2, but also provides the first conventional protection layer during the user key distribution.

However, instead of sending the once encrypted user key directly, a second protection layer with highly secure QKD keys is applied before transmission and provides the quantum-enhanced forward security of the user key distribution. Therefore, a fault tolerant dynamic routing algorithm based on the Dijkstra least cost path algorithm[24] first determines the optimal route of point-to-point QKD connections through the network, and chooses alternate routes and multiple paths when available in order to balance security and quality of service without the need of a centralized server. Using the secret symmetric QKD keys, which have been continuously established in parallel with the first intermediate node, the RSA encrypted user key is then additionally wrapped by an approved symmetric AES scheme and sent to the first intermediate node. Upon reception of this two-fold encrypted user key at the first intermediate node, the QKD-based symmetric encryption layer is first removed, and then re-applied but with the QKD keys which have been secretly shared between the first and the second intermediate node. Thus, the user key hops from node to node until reaching the final target node, where finally both the QKD-based protection layer and the RSA protection layer are removed, leaving the target node with the original user key for its use by an external device. Most importantly, the symmetric encryption layer with QKD keys ensures the quantum-safe forward security of the user key transmission, while in extension to other

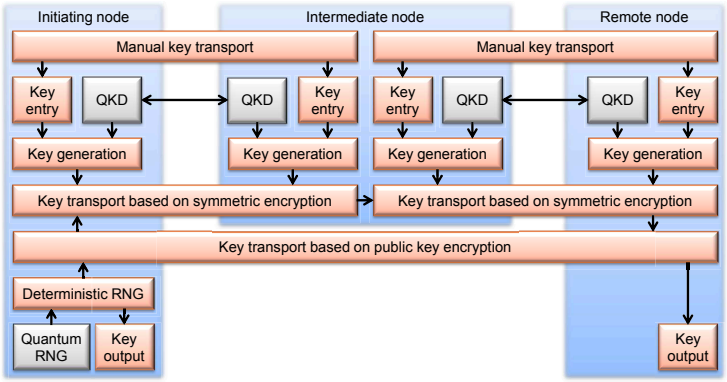


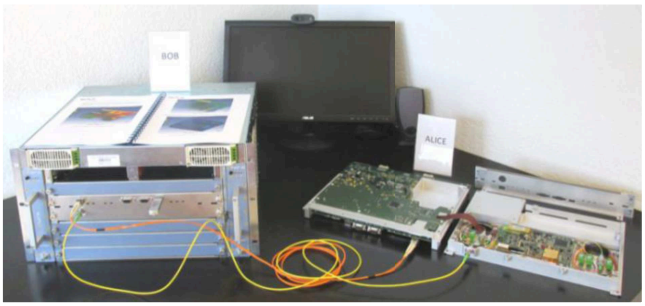
Figure 4. Illustration of the FIPS 140-2 approved methods used in the TN-QKD for secure key distribution between two users (see text for details).

trusted repeater QKD networks the RSA-based encryption layer maintains protection within intermediate nodes against insider attacks and facilitates compliance with the certification requirements.

For seamless integration into existing telecommunication infrastructure, the TN-QKD node hardware is implemented in the ATCA form factor,[15] a widely used telecom equipment specification standard that provides standardized mechanical, power and data interfaces, and a scalable architecture. Each individual node is housed in an ATCA shelf with a redundant Trusted Node Controller (TNC), and can be configured with multiple quantum blades depending on the desired network topology (see the photo in Fig. 5 left). The TNC provides administration interfaces, is responsible for node discovery, but most importantly provides route tables of the QKD network for routing and managing key transactions between blades within a node and with remote nodes. Depending on the number of adjacent nodes, each ATCA shelf node comprises several quantum blades which realize the QKD links and provide the cryptographic functionalities for securely distributing the user keys across the network. This flexible configuration of individual nodes allows implementing not only a simple chain network topology as exemplarily sketched in Figure 4, but any much more complex topology as required in a specific scenario while maintaining a small footprint. Each quantum blade comprises a quantum key engine (QKE) for the actual QKD links and quantum random number generation, and a quantum key controller (QKC). The QKC performs all cryptographic functions, and their required self-tests, which are necessary to securely send the user keys over the network as explained above. Such, the QKC realizes the key transport scheme, and the symmetric encryption and decryption with the QKD keys provided by the respective QKE. It also contains a high security memory and tamper detection module that stores all critical security parameters, including the quantum keys continuously provided by the QKE, in an encrypted memory and actively zeroizes them in response to a tamper detection.

While the principle architecture is independent of the underlying QKD protocol and allows adoption of different QKD systems in one network, our quantum key engine is based on a compact, 625 MHz clocked implementation of the coherent one-way (COW) QKD protocol (see[25] and references therein). It features an FPGA (field-programmable gate array) based key distillation engine, free-running single photon detector modules and quantum entropy sources, and is compatible with wavelength-division multiplexing technologies to operate, at minimum, over only one fiber. The FPGA-based key distillation engine uses a block size of 10^6 bit of sifted keys and allows secret key rates up to 4 Mbit/s. Real-time forward error correction is based on low-density parity-check codes, and privacy amplification uses universal hashing with Toeplitz matrices. The QKD service channel is Wegman-Carter authenticated, using QKD keys for one-time pad encryption of the authentication tags. The QKE post-processing employs the XOR method as explained in section 3.2 in order to render the QKD key compliant with the FIPS 140-2 requirements, while maintaining the information-theoretical security of the QKD keys. The shared seeds for the XOR method, along with the shared initial QKD authentication keys, are established using an approved key entry method during initialization. The total QKD security parameter*

*The security parameter quantifies the probability that a block of 10^6 bit of sifted keys results in an incorrect or



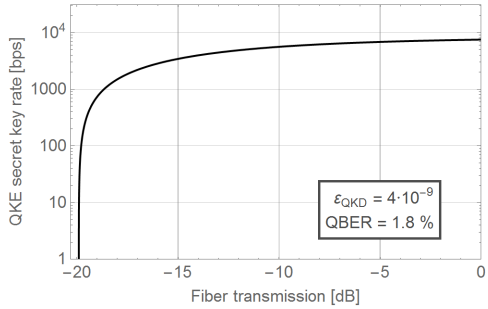


Figure 5. Left: Photo of the ATCA based TN-QKD node, configured with a single Bob quantum blade, and an opened Alice quantum blade with its quantum key controller and quantum key engine including all optical components.
Right: Results of the design validation for the ATCA quantum blades based on a quantum key engine implementing the COW QKD protocol. It allows for distribution of secret QKD keys of more than 1 kbit/s between adjacent nodes separated by over 90 km of standard telecom fiber, with a specified security parameter of $\varepsilon = 4 \cdot 10^{-9}$.

is specified as $\varepsilon = 4 \cdot 10^{-9}$.

A tamper-proof and -resistant hard metal enclosure with active zeroization response protects all cryptographic security functionalities within a quantum blade, including the QKE hardware. It's designed to support the thermal cooling of the interior components without the need for any openings, and to comply with the electromagnetic compatibility and interference requirements of FIPS 140-2. The front panel provides the interfaces for the user key output, the initialization, management and maintenance functions, and the optical fiber channels, with their access strictly separated and limited with respect to the specific authorized operator role as required by FIPS 140-2.

3.4 Results

Based on the described design we have performed preliminary lab tests of the QKE hardware with the results shown in the right of Fig. 5. For this test, an Alice and a Bob quantum blade were connected by two short fiber spools, one for the quantum channel and one for the QKD service channel, and the quantum channel attenuation was changed to simulate different fiber losses. As can be seen, despite their very compact design the quantum blades allow for distribution of secret QKD keys of more than 1 kbit/s between adjacent nodes separated by over 90 km of standard telecom fiber.

4. CONCLUSIONS AND OUTLOOK

In conclusion, we have described approaches and efforts toward quantum devices that are compliant with well-established security certification standards. As a first example, a quantum random number generator was certified to be compliant with the AIS 20/31 standard for random number generators. As a second example, we have described a Trusted-Node QKD system that was developed in compliance with the FIPS 140-2 certification standard for information security. Both these examples might pave the way for implementation of quantum technologies in environments that strictly require certification, and moreover increase attractiveness and trust in quantum technologies for their wider deployment.

REFERENCES

[1] Schindler, W., *AIS 20/AIS 31, Functionality classes for random number generators, ver. 2.0.* Federal Office for Information Security (BSI), Germany (2011).

[2] National Institute of Standards and Technology, Gaithersburg, MD, United States, *Federal Information Processing Standards (FIPS) Publications: FIPS 140-2, Security Requirements for Cryptographic Modules* (2002).

insecure output key.

[3] "ETSI QKD Industry Specification Group." www.etsi.org/technologies-clusters/technologies/quantum-key-distribution.

[4] The Common Criteria Recognition Agreement, *Common criteria for information technology security evaluation* (2012). (CCMB-2012-09-001, Ver. 3.1, Rev. 4).

[5] ID Quantique SA, "Quantis random number generator." http://www.idquantique.com/random-number-generation/quantis-random-number-generator/. [Online; accessed 31-July-2015].

[6] Barker, E. B. and Kelsey, J. M., *SP 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. National Institute of Standards and Technology, Gaithersburg, MD, United States (2012).

[7] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing," in [*Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*], 175–179, IEEE Press, New York (1984).

[8] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Reviews of Modern Physics* **74**(1), 145–195 (2002).

[9] Korzh, B. et al., "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics* **9**, 163–168 (Feb. 2015).

[10] Schmitt-Manderbach, T. et al., "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.* **98**, 010504 (2007).

[11] Natsheh, A. A., Gbadegeshin, S. A., Rimpiläinen, A., Imamovic-Tokalic, I., and Zambrano, A., "Identifying the challenges in commercializing high technology: A case study of quantum key distribution technology," *Technology Innovation Management Review* **5**, 26–36 (2015).

[12] Peev, M. et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics* **11**(7), 075001 (2009).

[13] Länger, T. and Lenhart, G., "Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD," *New Journal of Physics* **11**(5), 055051 (2009).

[14] Alléaume, R. et al., "Worldwide standardization activity for quantum key distribution," in [*Globecom Workshops, 2014*], 656–661 (2014).

[15] PICMG, *PICMG 3.0 Revision 2.0 AdvancedTCA Base Specification* (2008).

[16] Barker, E. B. and Roginsky, A., *SP 800-133. Recommendation for Cryptographic Key Generation*. National Institute of Standards and Technology, Gaithersburg, MD, United States (2012).

[17] http://www.battelle.org/our-work/national-security/cyber-innovations/quantum-key-distribution. [Online; accessed 31-July-2015].

[18] Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., and Yeh, H., "Current status of the DARPA quantum network (Invited paper)," in [*SPIE Conference Series*], *SPIE Conference Series* **5815**, 138–149 (2005).

[19] Stucki, D. et al., "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics* **13**(12), 123001 (2011).

[20] Mirza, A. and Petruccione, F., "Realizing long-term quantum cryptography," *J. Opt. Soc. Am. B* **27**, A185–A188 (Jun 2010).

[21] Chen, T.-Y. et al., "Metropolitan all-pass and inter-city quantum communication network," *Opt. Express* **18**, 27217–27225 (Dec 2010).

[22] Sasaki, M. et al., "Field test of quantum key distribution in the Tokyo QKD network," *Optics Express* **19**(11), 10387–10409 (2011).

[23] Wang, S. et al., "Field and long-term demonstration of a wide area quantum key distribution network," *Optics Express* **22**(18), 21739–21756 (2014).

[24] Dijkstra, E. W., "A note on two problems in connexion with graphs.," *Numerische Mathematik* **1**(1), 269–271 (1959).

[25] Walenta, N. et al., "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," *New Journal of Physics* **16**(1), 013047 (2014).