**Research article**

Francesco Raffaelli, Robert Denman, Richard Collins, Jean-Charles Faugere, Gaetano De Martino, Charles Shaw, Jake Kennard, Philip Sibson, Ludovic Perret and Chris Erven*

# Combining a quantum random number generator and quantum-resistant algorithms into the GnuGPG open-source software

https://doi.org/10.1515/aot-2020-0021
Received May 29, 2020; accepted September 14, 2020; published online October 22, 2020

**Abstract:** The "quantum threat" to our current, convenient cryptographic algorithms is getting closer, with demonstrable progress by commercial quantum computing efforts. It is now more important than ever that we combine all of our tools into a new quantum-safe toolbox to develop the next generation of quantum-safe networking solutions. Here we combine an integrated quantum entropy source with quantum-resistant algorithms in the GnuGPG open-source software; leading to a fully quantum-safe version of GnuGPG. The quantum entropy source itself is capable of a raw rate of randomness in excess of 10 Gbps. After post-processing, quantum random numbers are used by the quantum-resistant algorithms to allow GnuGPG to perform its usual public-key cryptographic tasks, such as digitally signing documents, but now in a secure quantum-safe way.

**Keywords:** post-quantum algorithms; quantum cryptography; quantum random number generator; quantum resistant algorithm; quantum-safe.

***Corresponding author: Chris Erven**, KETS Quantum Security Ltd., Unit DX, St. Philips Central, Albert Road, St. Philips, Bristol, BS2 0XJ, UK; and H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, Quantum Engineering Technology Labs, University of Bristol, Nanoscience and Quantum Information Building, Tyndall Avenue, Bristol, BS8 1FD, UK, E-mail: chris.erven@kets-quantum.com. https://orcid.org/0000-0001-6325-2668
**Francesco Raffaelli, Robert Denman, Richard Collins, Gaetano De Martino, Charles Shaw, Jake Kennard and Philip Sibson,** KETS Quantum Security Ltd., Unit DX, St. Philips Central, Albert Road, St. Philips, Bristol, BS2 0XJ, UK
**Jean-Charles Faugere and Ludovic Perret,** CryptoNext Security Ltd., 16 Boulevard Saint-Germain, Paris, 75005, France

## 1 Introduction

Quantum computing is no longer the stuff of science fiction. As it has moved from academic labs to commercial companies and start-ups it has started to make rapid, demonstrable progress. There are now multiple quantum computers from multiple different vendors hooked up to the cloud, ready to be programmed by physicists, corporate programmers and the general public. While this is great for advances in things like quantum chemistry and simulation, it also means that the "quantum threat" to our current cryptographic methods is getting closer by the day.

It has been known for more than three decades now that the mathematics protecting our current, number-theoretic based public-key cryptography algorithms can be broken by a quantum computer [1]. Indeed, although no classical polynomial-time algorithm has been found for integer factorization (FACT, which is used, for example, in the Rivest-Shamir-Adleman (RSA) algorithm) or the discrete logarithm problem ([DLOG], which is used for example, in Diffie-Hellman key-exchange); Shor's algorithm allows one to solve DLOG and FACT in polynomial-time on a quantum computer. Further, while initial estimates showed that one would need potentially millions of physical qubits to have enough high-quality error-corrected qubits to successfully run Shor's algorithm on public keys currently in use, recent work has drastically reduced the number of qubits required [2, 3].

We are now entering a phase where we must do something about it if we want to continue to use the vast e-commerce systems we have come to rely on. Luckily cryptographers, mathematicians, physicists and engineers have been hard at work on new quantum-safe cryptography methods. Quantum-safe cryptography is a suite of new cryptographic techniques which are believed to be immune to the threat of a quantum computer. They largely fall into two types: new quantum-resistant (QR) algorithms and quantum cryptography (QC) hardware (including quantum random number generators, QRNGs, and

quantum key distribution, [QKD]). QR algorithms (also called post-quantum cryptography) are based on different mathematical problems than those used in our current security methods which are thought to be secure from a quantum computer [4]. Whereas, QC bases its security on relating the operation of the device to the physical laws of nature [5].

Unfortunately, for almost equally as long as the two fields of QR and QC have existed, they have been arguing over which one is "right". We sidestep this argument, as we believe that this past approach suggesting a need to choose between QR and QC is a false dichotomy. In reality, true real-world cryptographic solutions are rich and complex, and QR and QC each give us new tools from which to build the next generation of secure cryptographic systems. Indeed, it is only by bringing all of our tools together that we will be able to move on to creating a wide array of new technologies and solutions which will bring with them a whole host of important, new questions to answer.

Trust models and chains of trust will become even more important as different parts of our complex networks use different tools to build up secure links. Upgrading legacy systems without breaking our networks and the enforced deprecation and retirement of insecure solutions will be key. For example, we will no longer be able to tolerate sectors like finance and banking still using Data Encryption Standard (DES) encryption decades after it was proven insecure.

Now is precisely the time to bring these and other technologies together into full solutions. The National Institute of Standards and Technology (NIST) in the US is currently running a competition to develop new QR standards which are expected in 2022[1]. In 2019, China[2] started a similar process and has already selected quantum-resistant algorithms. In parallel, the European Telecommunication Standards Institute (ETSI), the International Telecommunications Union (ITU-T), and the International Organisation for Standardisation (ISO) are developing new standards for QC hardware and adapting current security protocols (e.g. VPN, X.509, …) for a quantum-safe world.

Vendors are also preparing for the migration to new cryptographic standards. Now is the time to consider and build a framework for all quantum-safe cryptographic primitives. Crypto-agility, the ability to swap in and out different cryptographic technologies and solutions, is now the name of the game to ensure that we build our next-generation networks in a modular way such that we can always enjoy the highest levels of protection for our data.

To that end, this paper brings together QC hardware from KETS Quantum Security Ltd with CryptoNext Security Ltd's QR software library to develop a next-generation, quantum-safe version of the widely used open-source software: GnuGPG[3]. GnuGPG is an implementation of the OpenPGP standard and used as the security backbone for a multitude of applications and libraries including messaging and mailer applications. Here we show how to combine quantum random number generator and quantum-resistant software and incorporate it into the OpenPGP standard.

## 2 Quantum random number generator

Random numbers play a key role in cryptographic applications [6]. At the heart of almost any encryption system lies a source of randomness, which ultimately determines the security of the protocol itself. This is why methods to efficiently generate random numbers have been a key topic of research in the last few decades. Often, random numbers are produced by means of algorithms that expand a small random seed using symmetric cryptography algorithms that are generally thought to be quantum resistant (indeed these are many of the same algorithms that GnuGPG uses for bulk encryption and authentication, e.g. AES, HMAC, SHA-2). These are called pseudo random number generators (PRNGs).

While convenient, PRNGs have a main limitation. Once the algorithm and seed are known, it becomes straightforward to predict which numbers will be produced next. So if anyone gains knowledge of the random seed and how it is produced, the PRNG becomes easily predictable thus destroying its main purpose. This has drastic consequences for the security of any data encrypted using that PRNG since the first seed and any subsequent ones are now predictable, allowing the encrypted data to be easily decrypted. This is the specific threat model for our scenario. By replacing the PRNG (such as might be found in an Intel CPU) with a QRNG, we are ensuring that the randomness used in the QR algorithms in GnuGPG are truly random and unpredictable.

For the same reason the scientific community has invested remarkable efforts in developing true random number generators (TRNGs), where the randomness is the

1 https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.
2 http://sfjs.cacrnet.org.cn/site/term/list_77_1.html.
3 https://gnupg.org/.

result of a physical random event as opposed to a deterministic algorithm. Unfortunately, TRNGs also suffer from two main limitations. First, the randomness is often not due to an intrinsically probabilistic event, but rather a chaotic behaviour that is hard [7–9], but not impossible, to predict. Second, even when the source of randomness has an intrinsically quantum nature, as in the case of Ref. [10], it is often difficult to quantify the amount of entropy present in the system, distinguishing the true source of randomness from background noise of which little is known and/or it is difficult to control.

To solve these issues, quantum random number generators (QRNGs), which are based on the laws of quantum mechanics, have attracted the interest of the scientific community. Among these, optical QRNGs have proven to be very popular, due to the relatively easy and accessible early stage implementations. The first demonstration was proposed by Rarity et al. [11] which was based on measurements of strongly attenuated coherent light. Since then a wide range of QRNGs have been demonstrated, taking advantage of single photons [12–15]. Other techniques, based on optical phase fluctuations [16–19] and phase diffusion [16, 20, 21] have since been introduced to achieve randomness generation rates in the Gbps regime. Further methods take advantage of homodyne detection measurements of optical vacuum states which can provide high entropy rates and stronger guarantees around the quality of the generated entropy [22–25].

In the last few years QRNGs have been demonstrated in integrated Silicon-on-insulator technology [26–28] and InP [29]. Remarkably, these devices easily reach Gbps entropy generation rates and can be directly integrated into chip-based QKD systems [30, 31], which have been previously implemented in these integrated platforms.

One can also go to the opposite end of the spectrum and focus on cheaper QRNGs with slower randomness generation rates, and there is at least one commercial example of this [32]. These are also an interesting option which should continue to be explored. Each focuses on different applications. The slower and cheaper QRNG chip is very useful in lightweight applications, such as IoT (Internet of things) devices, while the high-speed QRNG chip discussed in this paper was designed with an eye to data centre and telecommunication use-cases that consume large quantities of randomness. Taken in isolation, this demonstration of an individual instance of performing quantum-safe digital document signing with GnuGPG could make use of slower and cheaper QRNG chips. However, our device was created as a scalable system resource, envisioning its installation in servers running hundreds even thousands of virtual machines, each themselves running multiple instances of applications utilising GnuGPG and other encryption algorithms requiring randomness. Taken in this context, it is clear why high-speed operation is a key benefit.

Here, we have implemented an improved version of Ref. [26] into a fully self-contained PCIe card, while increasing the generation rate by almost an order of magnitude. The QRNG is based on the homodyne detection measurement of optical vacuum states method, where the core optical measurements are performed on an integrated photonics device. Homodyne detection is a technique that enables the characterisation of optical quantum states in phase-space by interfering them with a strong coherent reference light signal called a local oscillator (LO) [33]. The LO and optical signal are interfered at a beam splitter and the outputs are detected by two photodiodes. The difference between the photocurrents generated by the photodiodes is proportional to the marginal distribution of the measured optical signal. The marginal distribution is the projection of the Wigner function on a certain angle in phase-space; namely, the angle given by the relative optical phase between the optical signal and LO. The marginal distribution therefore describes the probability that an optical system prepared in a well-defined quantum state (e.g. coherent state, squeezed state, etc) is measured to have a certain value. Hence, the outcome of each homodyne measurement is probabilistic and follows the marginal distribution.

Optical vacuum states, i.e. those states where no input optical signal is injected, can be used to generate random numbers and are characterised by a Gaussian marginal distribution. Here, each single homodyne measurement of a vacuum state has a random, normally distributed outcome. Remarkably, the only physical requirements of the optical apparatus for this type of QRNG are a coherent light source as an LO, a beam-splitting system, and two photodiodes. Further, this can be efficiently integrated onto photonic chips (see Figure 1), enabling one to reach very high entropy generation rates with a relatively simple, monolithically integrated system.

The most relevant parameters to describe the performance of the QRNG are the 3 dB bandwidth of the homodyne detector and the signal-to-noise clearance (SNC) between the quantum optical shot-noise and the background electronic noise. In Figure 2 we show a sample of the spectral power density as measured during the characterisation of the device prior to its use. Here we can observe a bandwidth of 1 GHz and an SNC above 10 dB across the bandwidth of interest.

The SNC determines the amount of randomness extractable which is quantified by the min-entropy. In this

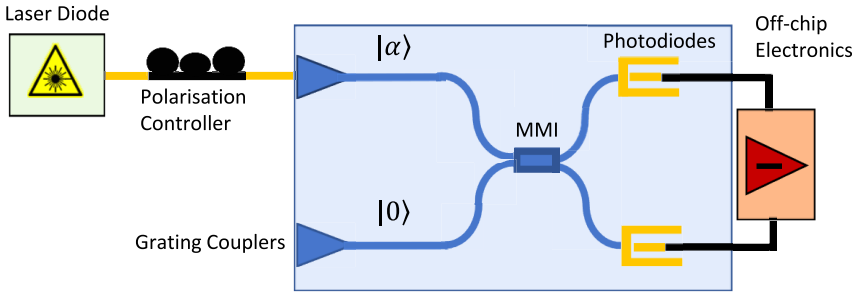


**Figure 1:** Optical homodyne detector. The optical apparatus consists of an off-chip laser diode connected to the chip through a polarisation controller. An integrated beam-splitter MMI is used to combine the LO and optical vacuum. Two on-chip, high-speed photodiodes convert the optical signals into photocurrents that are further processed by off-chip electronics.

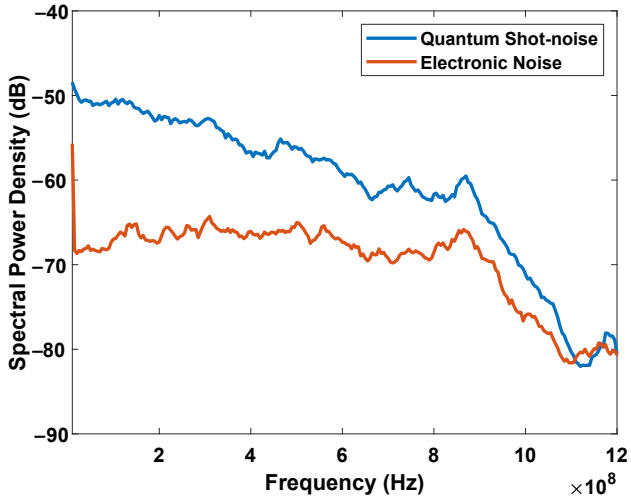


**Figure 2:** Spectral Density of the shot-noise. The optical quantum shot-noise (blue line) has a bandwidth of at least 800 MHz and a clearance from the electronic noise above 10 dB in the entire bandwidth of interest. Given the 1.6 Gsa/s sampling rate of our analogoue-to-digital converter, 800 MHz is an optimal bandwidth to minimize the autocorrelation of the quantum signal.

demonstration, we worked under the assumption of a fully-trusted device for our QRNG. This means that we assume we have an accurate physical model of the device that has been vetted by a third party, and the device is in our control in a trusted environment (for instance, in the secure enclosure of a data centre server). From this, the characterisation of the device then follows a similar approach as in Ref. [26] and described in more detail in Ref. [34].

The min-entropy $H_\infty(X)$ is defined as

$$H_\infty = -\log_2\left(\max_{x\in\{0,1\}^n} \Pr[X = x]\right), \tag{1}$$

where $X$ is a distribution and $x$ an n-bit string. One of the great advantages of the min-entropy is that it can be interpreted as the number of uniform bits that can be extracted from a given distribution [35, 36], as shown in Ref [34], and it can be used to perform theoretically proven randomness extraction.

In this implementation we used a software version of the Toeplitz extractor to generate a uniform distribution seeded by the normal distribution obtained from the raw digitised optical measurements. The role of the Toeplitz extractor is two-fold. It takes a normally distributed bit-string of a given min-entropy and turns it into a uniformly distributed bit-string whose length is related to the min-entropy itself. And it removes any residual biases present in the raw data, biases that could be due to a non-infinite SNC or imperfections of the electronics hardware.

Using Eq. (1), we obtained $H_\infty \geq 9$ when using a 12 bit ADC. Given the sampling rate of 1.6 Gsamples/s, this shows the potential for generation rates in excess of 10 Gbps, provided fast enough post-processing. For this demonstration, however, we used a software based post-processing routine, strongly limiting the generation rate which was nonetheless sufficient for the purposes of this demonstration. Because of the fully-trusted scenario, our system constantly monitored all of the most relevant physical parameters in order to assure security.

Eq. (1) is valid under the assumption that the quantum noise can be distinguished from the classical sources of noise, such as the electronic noise. In the case of a QRNG based on homodyne measurements of optical vacuum states, the voltage signal output from the homodyne detector (and digitised by the analogue-to-digital converter) has a Gaussian distribution. The electronic noise intrinsic to the system components also has a Gaussian distribution, while environmental noise can potentially have different kinds of distributions and spectrums. The QRNG system must be isolated from both of these noise sources. By periodically monitoring the output voltage signals when the laser is on and compared to when the laser is off, we constantly check that our assumptions about the distribution of quantum signal and noise floor are valid.

Moreover, the quantum shot-noise of optical vacuum states grows linearly with the optical power of the local oscillator. This is in opposition with the intensity noise of the laser that grows with the square of the input optical power. Hence, by periodically selecting different values of

optical power, we check that the signal observed has the expected linear behaviour. A failure in any these two checks implies insecure random numbers and the data collection of the QRNG is interrupted and random number output is stopped.

Furthermore, in this particular implementation the laser source is connected to the integrated photonic chip through single mode fibres. Therefore a fibre in-line digital polarisation controller is used to maximise the optical power coupled onto the integrated device. Given that the optical decoupling due to polarisation shift is observed to be well below 0.1 dB/s, we provide a feedback loop on the polarisation at the pace of one loop per minute. This is sufficient to maintain polarisation stability during the time period of the demonstration (usually up to a few hours). Other parameters such as temperature stability and power consumption are always kept under control as a change in these would imply a potential failure of the system and therefore reduction of the quality of the generated random data. The temperature in particular is kept stable with thermo-electric control of the chip with the use of a Peltier module and a PID loop.

## 3 Quantum-resistant algorithms

Quantum-resistant cryptography [4] deals with the design of cryptographic primitives which are secure against classical and quantum adversaries. This is a well established academic topic mainly motivated by Shor's milestone quantum factoring algorithm [1]. A fundamental assumption in quantum-resistant cryptography is that there is no polynomial-time algorithm for solving any NP-Complete problem (see for example Ref. [37]), giving confidence in the existence of cryptographically interesting problems that are hard to solve in the quantum setting.

The status of quantum-resistant cryptography has completely changed in the last few years. With the advances of quantum computing, it has quickly moved from a purely academic theme to a topic of major industrial interest. In particular, QR cryptography has recently received much attention from the standardization and policy spectra with many activities on post-quantum cryptography flourishing in world-wide standards bodies, including: ETSI, ISO, and IETF.

The most prominent standardisation activity is being done by NIST, which has the authority to produce security standards for the US government. In January 2016 they released a call to select standards for post-quantum public-key cryptosystems including: Key encapsulation mechanisms (KEM) and signatures. With historical perspective, for example with the advanced encryption standard (AES), it seems likely that the QR standards derived from this process will be widely endorsed around the world.

At the time of writing this paper, NIST is at the end of the second round of its QR standardization process. Initially, NIST received 82 submissions (23 signature schemes and 59 encryption/KEM schemes). The second round started mid-2019 and narrowed down the number of candidates to nine signatures and 17 KEMs. The intention of NIST is not to take a single winner for each category but to select several candidates. The main reason is that quantum-resistant algorithms have different practical features compared to currently deployed public-key cryptosystems. As a consequence, different quantum-safe resistant algorithms are optimal for different applications.

Quantum resistant cryptography mostly focuses on six different approaches: lattice-based, multivariate, hash-based, code-based, supersingular elliptic curve isogeny and symmetric key. The most popular approaches to meeting the NIST requirements are the lattice and code based methods (note AES, which is commonly used to encrypt large amounts of data, falls into the symmetric key approach and is thought to be quantum-safe). The quantum-resistant cryptography library used in this demonstration has been designed to include the vast majority of the different NIST quantum-resistant candidates in order to give users the ability to optimise for their particular application. For this quantum-safe GnuGPG digital document signing demo we used the proprietary libcns algorithm which is a lattice-based method.

## 4 The quantum-safe GnuGPG demo

The quantum-safe GnuGPG demo was designed to show how a QRNG can be used to seed a QR software algorithm which can then be used inside GnuGPG. The ultimate security of cryptographic algorithms, including post-quantum algorithms, relies on the source of randomness used to seed the algorithms and the correct implementation of the algorithm itself. As mentioned in Section 2, we characterise the quality of the data from the QRNG in two ways. Firstly, the *quantumness* of the data is estimated based on our quantum mechanical model of our device. Secondly, because of the imperfections that might incur in an actual implementation of the hardware device, the data is also checked from a statistical point of view using the NIST statistical test suite [38]. Figure 3 shows the output of the NIST test suite for a sample of data from our QRNG.

The design of the system (Figure 4) shows how we combined the QRNG with a software interface that allowed

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <qrng_data_V2>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
184 196 184 229 208 185 213 225 192 184  0.127393   1981/2000    Frequency
177 182 186 237 201 222 202 214 185 194  0.051611   1977/2000    BlockFrequency
189 192 203 185 213 221 228 190 171 208  0.119160   1985/2000    CumulativeSums
216 202 185 224 185 221 184 189 190 204  0.268917   1978/2000    Runs
177 206 200 231 183 216 190 199 199 199  0.284725   1983/2000    LongestRun
195 201 182 200 184 171 199 215 230 223  0.077846   1974/2000    Rank
205 218 213 188 194 220 189 206 187 180  0.426272   1975/2000    FFT
195 199 194 208 177 203 199 216 230 179  0.255057   1985/2000    NonOverlappingTemplate
218 211 188 203 189 206 222 193 200 170  0.279844   1970/2000    OverlappingTemplate
219 221 167 209 193 229 190 191 182 199  0.051281   1984/2000    Universal
208 209 204 185 195 171 214 198 216 200  0.480771   1977/2000    ApproximateEntropy
128 140 115 123 131 119 126 135 111 123  0.770693   1241/1251    RandomExcursions
118 112 121 130 134 121 136 132 130 117  0.841226   1240/1251    RandomExcursionsVariant
191 197 194 188 203 204 178 193 218 234  0.240501   1980/2000    Serial
221 202 210 174 208 175 195 183 205 227  0.094002   1976/2000    LinearComplexity


- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 1966 for a
sample size = 2000 binary sequences.

The minimum pass rate for the random excursion (variant) test
is approximately = 1227 for a sample size = 1251 binary sequences.

For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

**Figure 3:** NIST Test Results on a 2 Gb Data Sample.
The NIST test [38] divides the set of data into 2000 1 Mb sub-blocks. Each of the 15 tests, reported in the right column is applied to each sub-block. The proportion of sub-blocks that passed the test is reported on the second column from right, and in order for a test to be considered successful, the proportion must be above a given threshold, as described above. The columns C1–C10 report the number of times a *P*-value is measured within a certain interval. C1 for *P*-values between 0 and 0.1, C2 for *P*-values between 0.1 and 0.2 etc. The column called *P*-value reports the *P*-value of the distribution of the *P*-values collected from the tests on each single sub-block, and it is relative to the null hypothesis that these *P*-values follow a uniform distribution. Uniformly distributed *P*-values imply that the null-hypothesis was verified.

it to be used as a source of randomness in the QR software library which was then itself integrated into GnuGPG. It was designed in several discrete sections: the quantum entropy board, a board containing the QRNG and supporting hardware with an on-board microprocessor for hardware calibration and monitoring; the data capture board, a propriety board that allows for use of a high speed ADC to convert the analogue entropy into a digital format; the QRNG Software Suite, software that controls the overall state of the system, calibrates the system, processes the entropy data into random data and monitors the entropy data coming from the data capture board while also providing an interface to external sources to access the random data; and finally the GnuGPG suite which takes the random data generated from the rest of the system and uses it as a way of seeding the QR algorithms to digitally sign documents.

The system boots with initialisation and calibration steps beginning by measuring the noise floor with the laser off and on in order extract the randomness due purely to the quantum mechanical effects. It also maximises the optical power coupled into the device by adjusting the in-line digital polarisation controller. It then measures the linearity of the noise variance by stepping through different optical optical powers. Finally, all of this information, plus knowledge of the physical model of our device, are used to calculate the min-entropy from Eq. (1) in order to tell the system how much randomness can be generated. A random Toeplitz matrix is generated each run by saving a small amount of randomness from the previous run.

Figure 5 shows the GnuGPG agent incorporating the QR library and the QRNG where the interfaces remain unchanged. Displayed is a generated hybrid certificate consisting of the digital document being signed twice, once with a classical signature (RSA) and then with the quantum-resistant signature. It is worth noting that hybridisation techniques is a rich subject with many proposals, for instance, see Refs. [39–44]. The overall GnuGPG document signing application had an almost identical run time when it pulled entropy from the QRNG as opposed to the usual internal PRNG call. This is as expected since the QRNG was only required to generate small initial seeds that were either 128, 192 or 256 bits. When doing the hybrid signature (i.e. the combined classical and quantum-resistant signatures) the program was marginally slower, on the order of milliseconds, which is not expected to make a substantial difference to the end-user.

The security of the entire scheme relies then on the randomness of the QRNG (verified on one hand through real-time monitoring of the physical parameters and on the other hand by applying statistical tests, such as those of the standard NIST suite shown in Figure 3, to samples of generated random bits), the hardness of FACT (RSA), and

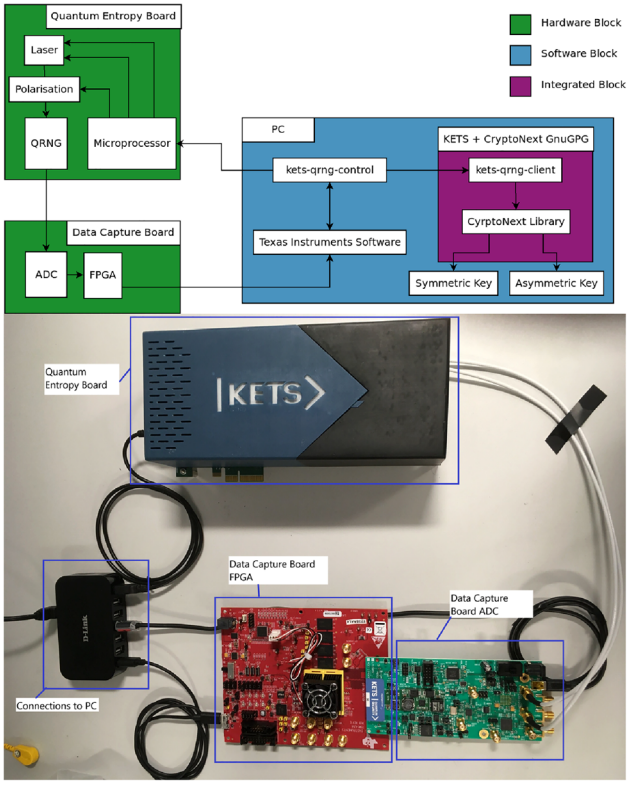


**Figure 4:** Design of the System.
A block diagram showing the relationship of individual components and the flow of information through the system (top). The setup of the system annotated with reference to the design diagram (bottom). The quantum entropy board provides the data capture board with analogue entropy which is converted into a digital representation using the ADC and FPGA. This is then collected by the software on the PC and processed into random bits which are stored until they are requested by the client. When requested, they provide the seed for the QR algorithms in order to digitally sign a document or produce a key.

the hardness of breaking the libcns quantum-resistant algorithm. This is in line with the many international bodies and governments which are advising industry to make the migration to a quantum-safe world in such a way that is backwards compatible by not immediately replacing current cryptography but rather increasing its security in a hybrid mode.

## 5 Outlook and conclusions

In conclusion, this work has shown how to bring together multiple different new quantum-safe tools; namely, quantum random number generation and quantum resistant algorithms, in order to make the widely used GnuGPG implementation of the OpenPGP cryptographic standard quantum-safe. We did so while continually monitoring a number of security parameters of our device in order to ensure the security of the entropy it generated. The use of the QRNG compared to the usual PRNG used did not noticeably affect the performance of the system.

This demonstration is a crucial step in recognising the rich new quantum-safe toolbox consisting of both quantum resistant algorithms and quantum cryptography hardware now available to us to build the next generation of secure cryptographic systems. As we continue to increase our reliance on networked information systems it is important that we continue to prepare and be ready for emerging threats to our current cryptographic techniques, such as quantum computers, so that we can properly migrate to quantum-safe systems and ensure the integrity and security of the data in those systems.

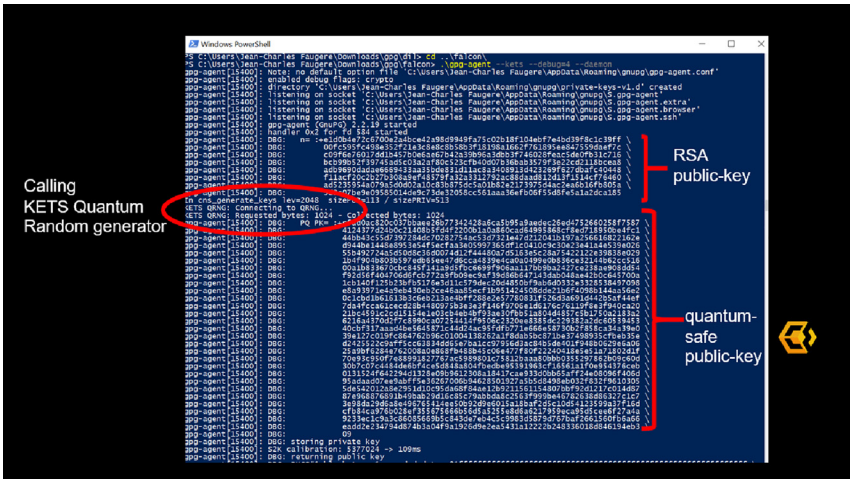


**Figure 5:** GnuGPG Quantum-Safe Key Generation.
GnuGPG using the QR algorithm to generate a quantum safe public key/private key pair, seeded with 1024 bytes of QRNG data.

Remote working is steadily becoming the norm and many critical information systems absolutely need to be upgraded and made quantum-safe as the attack surface has now grown exponentially to include all of our homes. We will require remote quantum-safe software repositories, remote quantum-safe asset diagnostics and repair, and remote quantum-safe engineering design tools. Far from being the end of the story, combining QR and QC tools will open a host of important new questions to answer while we build quantum-safe chains of trust in our twenty first century information technology systems.

**Author contribution**: All the authors have accepted responsibility for the entire content of this submitted manuscript and approved submission.
**Research funding**: None declared.
**Conflict of interest statement**: The authors declare that they are employed at 2 start-ups which produce commercial QRNG and QR solutions.

## References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.
[2] V. Gheorghiu and M. Mosca, *Benchmarking the Quantum Cryptanalysis of Symmetric, Public-Key and Hash-Based Cryptographic Schemes*, arXiv:1902.02332 [quant-ph], 2019.
[3] E. Anschuetz, J. Olson, A. Aspuru-Guzik, and Y. Cao, "Variational quantum factoring," in *Quantum Technology and Optimization Problems* Cham, S. Feld and C. Linnhoff-Popien, Eds., New York, Springer International Publishing, 2019, pp. 74–85.
[4] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, pp. 188–194, Sept 2017.
[5] S. Pirandola, U. L. Andersen, L. Banchi, et al., *Advances in Quantum Cryptography*, arXiv:1906.01645 [quant-ph], 2019.
[6] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, p. 015004, Feb 2017.
[7] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.*, vol. 103, p. 024102, Jul 2009.
[8] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators. Part II: practical realization," *IEEE Trans. Circ. Syst. Fund. Theor. Appl.*, vol. 48, pp. 382–385, March 2001.
[9] J. Szczepanski, E. Wajnryb, J. Amigo, M. V. Sanchez-Vives, and M. Slater, "Biometric random number generators," *Comput. Secur.*, vol. 23, no. 1, pp. 77–84, 2004.
[10] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Circ. Syst. Fund. Theor. Appl.*, vol. 47, pp. 615–621, May 2000.
[11] J. Rarity, P. Owens, and P. Tapster, "Quantum random-number generation and key sharing," *J. Mod. Optic.*, vol. 41, no. 12, pp. 2435–2444, 1994.
[12] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Rev. Sci. Instrum.*, vol. 71, no. 4, pp. 1675–1680, 2000.
[13] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, "Photon arrival time quantum random number generation," *J. Mod. Optic.*, vol. 56, no. 4, pp. 516–522, 2009.
[14] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Appl. Phys. Lett.*, vol. 98, no. 17, p. 171105, 2011.
[15] M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Rev. Sci. Instrum.*, vol. 78, no. 4, p. 045104, 2007.
[16] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Optic. Lett.*, vol. 35, pp. 312–314, Feb 2010.
[17] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Optic. Express*, vol. 20, pp. 12366–12377, May 2012.
[18] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Rev. Sci. Instrum.*, vol. 86, no. 6, pp. 063105, 2015.
[19] J. Liu, J. Yang, Z. Li, et al., "117 gbits/s quantum random number generation with simple structure," *IEEE Photon. Technol. Lett.*, vol. 29, pp. 283–286, Feb 2017.
[20] M. Jofre, M. Curty, F. Steinlechner, et al., "True random numbers from amplified quantum vacuum," *Optic. Express*, vol. 19, pp. 20665–20672, Oct 2011.
[21] C. Abellán, W. Amaya, M. Jofre, et al., "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Optic. Express*, vol. 22, pp. 1645–1654, Jan 2014.
[22] C. Gabriel, C. Wittmann, D. Sych, et al., "A generator for unique quantum random numbers based on vacuum states," *Nat. Photon.*, vol. 4, pp. 711–715, Oct 2010.
[23] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, *Secure Heterodyne-Based Quantum Random Number Generator at 17 Gbps*, arXiv:1709.00685v1 [quant-ph], 2017.
[24] B. Xu, Z. Li, J. Yang, et al., *High Speed Continuous Variable Source-independent Quantum Random Number Generation*, arXiv:1709.00685v1 [quant-ph], 2017.
[25] Z. Zheng, Y.-C. Zhang, W. Huang, S. Yu, and H. Guo, *6 Gbps Real-Time Optical Quantum Random Number Generator Based on Vacuum Fluctuation*, arXiv:1805.08935 [quant-ph], 2018.
[26] F. Raffaelli, G. Ferranti, D. H. Mahler, et al., "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," *Quant. Sci. Technol.*, vol. 3, no. 2, p. 025003, 2018.
[27] F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, and J. C. F. Matthews, "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," *Optic. Express*, vol. 26, pp. 19730–19741, Aug 2018.
[28] M. Rude, C. Abellan, A. Capdevila, et al., *Phase Diffusion Quantum Entropy Source on a Silicon Chip*, arXiv:1804.04482 [quant-ph], 2018.

[29] C. Abellan, W. Amaya, D. Domenech, et al., "Quantum entropy source on an photonic integrated circuit for random number generation," *Optica*, vol. 3, pp. 989–994, Sep 2016.
[30] P. Sibson, C. Erven, M. Godfrey, et al., "Chip-based quantum key distribution," *Nat. Commun.*, vol. 8, p. 13984, Feb 2017.
[31] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," *Optica*, vol. 4, pp. 172–177, Feb 2017.
[32] Quantis QRNG chip, 2020. Available at: https://www.idquantique.com/random-number-generation/products/quantis-qrng-chip.
[33] A. I. Lvovsky and M. G. Raymer, "Continuous-variable optical quantum-state tomography," *Rev. Mod. Phys.*, vol. 81, pp. 299–332, Mar 2009.
[34] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction," *Phys. Rev.*, vol. 87, p. 062327, Jun 2013.
[35] B. Chor and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity," *SIAM J. Comput.*, vol. 17, no. 2, pp. 230–261, 1988.
[36] D. Zuckerman, "General weak random sources," in *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science, St. Louis, MO, USA, IEEE Institute of Electrical and Electronics Engineers*, 1990, pp. 534–543.
[37] C. H. Bennett, E. Bernstein, G. Brassard, and U. V. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1510–1523, 1997.
[38] A. Rukhin, J. Soto, J. Nechvatal, et al., *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Gaithersburg, MD, USA: National Institute of Technology, 2010.
[39] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a quantum-resistant public key infrastructure," in *PQCrypto 2017. Lecture Notes in Computer Science*, vol. 10346, T. Lange and T. Tsuyoshi, Eds., Cham, Springer, 2017, pp. 384–405.
[40] P. Kampanakis, P. Panburana, E. Daw, and D. V. Geest, *The viability of post-quantum x.509 certificates*, Cryptology ePrint Archive, Report 2018/063, 2018. Available at: https://eprint.iacr.org/2018/063.
[41] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Post-quantum authentication in tls 1.3: a performance study," in *Network and Distributed Systems Security (NDSS) Symposium 2020*. St. Louis, USA: NDSS; 2020.
[42] N. Bindel, J. Braun, L. Gladiator, T. Stöckert, and J. Wirth, "X.509-compliant hybrid certificates for the post-quantum transition," *J. Open Source Software*, vol. 4, no. 40, p. 1606, 2019.
[43] Composite keys and signatures for use in internet PKI, 2020. Available at: https://tools.ietf.org/html/draft-ounsworth-pq-composite-sigs-02.
[44] ISARA catalyst agile digital certificate technology, 2020. Available at: https://www.isara.com/products/isara-catalyst-agile-digital-certificate-technology.html.