npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Quantum random number cloud platform

Leilei Huang[1]✉, Hongyi Zhou[2], Kai Feng[1] and Chongjin Xie[1]

Randomness lays the foundation for information security. Quantum random number generation based on various quantum principles has been proposed to provide true randomness in the last two decades. We integrate four different types of quantum random number generators on the Alibaba Cloud servers to enhance cybersecurity. Post-processing modules are integrated into the quantum platform to extract true random numbers. We employ improved authentication protocols where original pseudo-random numbers are replaced with quantum ones. Users from the Alibaba Cloud, such as Ant Financial and Smart Access Gateway, request random numbers from the quantum platform for various cryptographic tasks. For cloud services demanding the highest security, such as Alipay at Ant Financial, we combine the random numbers from four quantum devices by XOR the outputs to enhance practical security. The quantum platform has been continuously run for more than a year.

npj Quantum Information (2021)7:107 ; https://doi.org/10.1038/s41534-021-00442-x

INTRODUCTION

Random numbers play an important role in cybersecurity, cryptography, lottery, and scientific simulations[1–3]. In recent years, with the widespread of next-generation information technologies such as big data, cloud computing, and Internet of Things, a large amount of confidential data related to customer privacy has been increasingly exposed to the Internet. Data security is facing great challenges from increasing computing power, future quantum computers, and new-algorithm attacks[4,5]. In the meantime, poor implementations of randomness generation would open up serious security loopholes for cryptosystems even when the underlying algorithms are secure[6–10]. Even for those newly proposed lattice or hashed-based quantum-safe cryptography algorithms, randomness is still a fundamental problem that cannot be solved with classical means. The ability to provide high-quality, high-speed, and stable random number services is an essential demand for information security today[11,12].

Quantum random number generators (QRNGs) have attracted extensive interests in the past two decades. For a review of the subject, please refer to the recent review articles[13,14] and references therein. The essential difference between QRNGs and classical ones (such as pseudo or thermal noise-based) lies in the unpredictability[15,16]. Guaranteed by the principle of quantum mechanics, QRNGs can avoid predictability loopholes in classical random numbers. As a result, quantum devices show the superiority in tasks with a high information security level, such as data encryption, authentications, and digital signatures. Till now, various methods have been applied to generate quantum randomness, such as detecting the path of a single-photon after a beam splitter[17–19], the arrival time of a weak coherent state[20–24], the photon-counting detection or the vacuum-fluctuations of an optical field[25–29], and the phase fluctuations in spontaneous emission[30–33]. Moreover, when we relax the assumptions and characterizations on the devices, there are also device-independent[34,35] and semi-device-independent QRNG schemes[36,37].

With so many different choices of QRNGs, it is challenging for end-users to understand the underlying principles and to get familiar with various physical and application programming interfaces (APIs) of different devices. Besides, no universal QRNG standards and verification techniques have been officially released so far, making it difficult to evaluate the quality and performance of QRNGs. Individual QRNG devices are usually lack of real-time randomness check, and cannot provide sustainable random number services to online security applications with high stability request. A high-quality quantum random number service should be adaptive with various QRNGs using different interfaces and plug-and-play even if any (not all) device fails.

In this work, we realize a platform on the Alibaba Cloud servers that provides random numbers from four different types of QRNGs, including those based on single-photon detection, photon-counting detection, phase-fluctuations, and vacuum-fluctuations. Real-time post-processing and randomness monitoring modules are integrated into the platform. The generated random numbers are fed into applications either on the Alibaba Cloud servers or remote access for data encryption, with various security levels and speeds. For applications in financial services requiring the highest security, we combine the random numbers from the four quantum devices by bitwise exclusive-*OR* of the outputs. In this case, as long as at least one of the devices provides true randomness, the applications are secure. A universal trust-cloud-center is more reliable than individual device manufactures. In practice, it is much more challenging for hackers to find loopholes in all different QRNGs. In the future, we would add more quantum entropy sources into the systems to further enhance the security on the implementation level.

RESULTS

Platform realization

Recently, popular QRNG realizations are mainly based on single-photon detection, photon-counting detection, and phase or vacuum-fluctuations. The schematic diagram of each principle is shown in Fig. 1. The most straightforward idea of QRNG is based on single-photon detection, as shown in Fig. 1(a). When a photon passes through a 50/50 beam splitter, the probabilities to enter detector "0" and detector "1" are balanced[17–19]. Due to the dead time of single-photon detectors, such QRNGs usually have a limited speed of Mbps, while phase-fluctuation ones[30–33] in Fig. 1(b) can dramatically increase the generation speed up to Gbps using traditional photodetectors. Due to the complexity of their optical

[1]Alibaba Cloud Intelligence Business Group, Alibaba Group, Hangzhou, China. [2]Photon Science Center, Graduate School of Engineering, The University of Tokyo, Tokyo, Japan. ✉email: hll187188@alibaba-inc.com

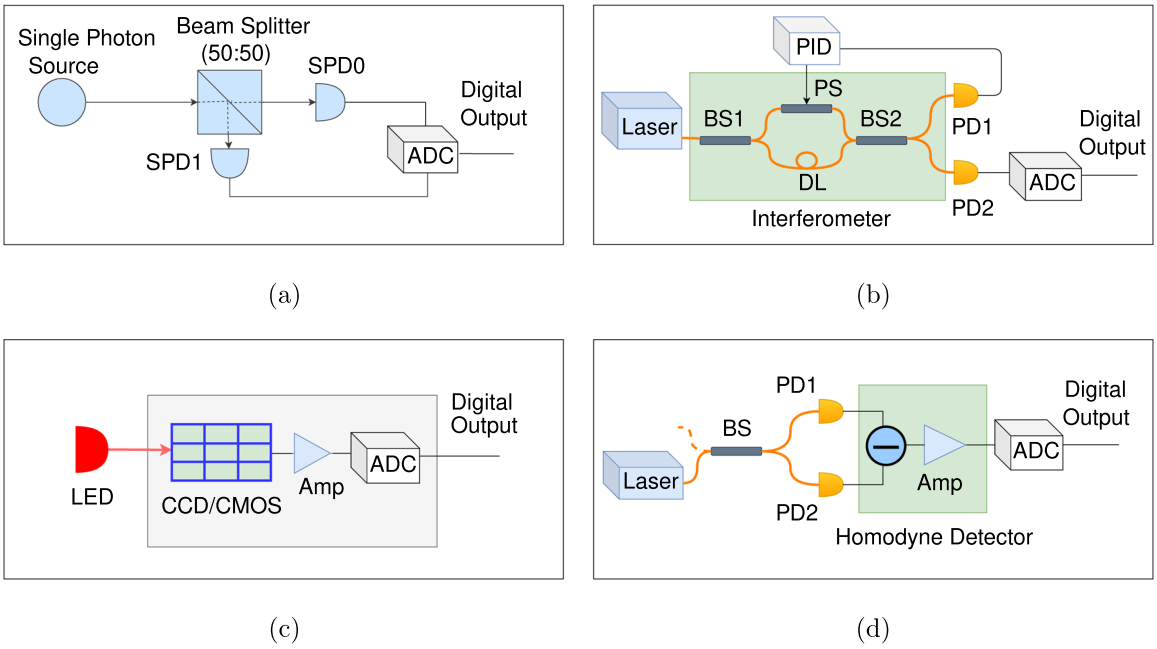

Fig. 1 Schematic diagram of QRNG devices based on various quantum principles. BS: beam splitter 50/50, PD: photodetecotr, SPD: single-photon detector, ADC: analogue to digital converter, PID: proportional-integral-derivative control, PS: phase-shifter, DL: delay line, Amp: amplifier. **a** Single-photon-detection QRNG. **b** Phase-fluctuation QRNG. **c** Photon-counting-detection QRNG. **d** Vacuum-fluctuation QRNG.

setups, commercial phase-fluctuation QRNGs are normally bulky (approximately in the size of 1U rack). A more compact QRNG-chip (Fig. 1(c)) based on photon-counting detection[25] has been demonstrated and commercialized, with a relative simple setup and moderate generation rate (240 Mbps). However, the theoretical evaluation of classical and quantum entropy for direct photon-counting QRNGs is still under discussion. For comparison and easy demonstration, a lab-made vacuum-fluctuation QRNG[26–28] has also been demonstrated in Fig. 1(d) with a generation rate of 400 Mbps (limited by the characteristics of the homodyne detector), where the lab-made homodyne detector has a bandwidth of 150 MHz and a common mode rejection ratio of 30 dB. All the types of QRNGs above are adopted by our platform.

We present the QRNG Platform protocol and the schematic diagram of the platform setup is shown in Fig. 2. Details of the QRNG cloud platform protocol are described as follows.

1. **Data import**. The cloud platform adopts quantum random numbers from various QRNG devices through different interfaces (e.g., PCIe, USB, Ethernet, etc.). Our online random number server provides standard interfaces (RESTful or gRPC API), or random numbers can be downloaded from website directly for end-users. The request size of random numbers can be customized, and APIs are compatible with multiple data format including binary, text, ASCII, etc.
2. **Randomness extraction**. The randomness of the input random numbers from different entropy sources are evaluated. The random numbers pass a real-time randomness extractor, by which the randomness per bit is enhanced to almost 1.
3. **Bitwise XOR**. A bitwise XOR operation is performed between random numbers from two or more quantum entropy sources. For each train of n-bit random series $X_i(n)$, the output random train $Y(n)$ is given by
$$Y(n) = X_1(n) \bigoplus X_2(n) \bigoplus X_3(n) \bigoplus \cdots \quad (1)$$
This step is optional.
4. **Randomness test**. The platform performs regular (upon request, hourly by default) real-time entropy estimation test (NIST SP 800–90B) to evaluate the non-IID entropy of the quantum random sources, as well as standard NIST randomness test (NIST-800–22) to verify the quality and status of the generated random numbers.
5. **Identity authentication**. The cloud server performs identity authentication with the end-users upon requests, using pre-shared key (PSK).
6. **Data download**. End-users download random numbers in plaintext or ciphertext with classical encryption protocols (such as secure socket layer and transport layer security, SSL/TLS) according to the their needs.

Here are some remarks for the protocol. First, we integrate a real-time post-processing into our cloud. The post-processing technique, namely a randomness extractor (k, ϵ, n, d, m)-extractor, is a function

$$\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m \quad (2)$$

that transforms the n-bit raw sequence with conditional min-entropy $H_{min}(\rho_A|E) \geqslant k$ (this quantity characterizes the true randomness of ρ_A in the presence of eavesdroppers E) to a m-bit sequence arbitrarily close to a uniform distribution with the help of a d-random-bit seed. This process will succeed with a probability no $<1-\epsilon$. The relations of these parameters are given by the Leftover Hash Lemma

$$m \leq nH_{min}(\rho_A|E) - 2\log_2\left(\frac{1}{\epsilon}\right) \quad (3)$$

For different QRNGs, we quantify the randomness and apply corresponding extractors according to $H_{min}(\rho_A|E)$ and get uniform output sequences. In our implementation, both commercial and lab-made QRNG devices are connected to the QRNG Platform. For the commercial QRNGs, the conditional min-entropy is evaluated internally with real-time post-processing by the devices. For the lab-made QRNG, we assume that the quantum signal and classical noise follow independent Gaussian distributions[29] in the strong local oscillator limit, and we have the following relation about their variances,

$$\sigma_t^2 = \sigma_q^2 + \sigma_c^2. \quad (4)$$

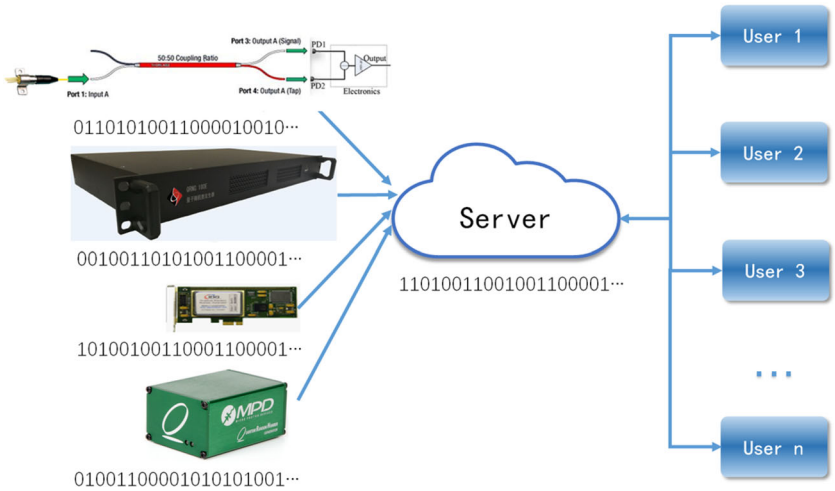

Fig. 2 Schematic Diagram of the QRNG Cloud Platform. Redundant backup server and QRNG devices are provided in different server rooms in case of system corruptions.

σ_t is the standard deviation of the output of the ADC, which includes both σ_q (quantum signal) and σ_c (classical noise). In a QRNG whose devices are trusted and characterized, the conditional-min entropy is calculated by extracting the quantum signal from classical noise.

Here we take a vacuum-fluctuation QRNG as an example. The fundamental quantum randomness comes from the shot noise of the coherent laser source, whose variance σ_q^2 is a linear function of the intensity of the local oscillator[38]. The classical noises are assumed to be independent with laser power[26–29], which can be obtained in the absence of the local oscillator. Then we can calculate the signal-to-noise ratio at a certain laser power,

$$\gamma = 1 - \frac{\sigma_c^2}{\sigma_t^2} \tag{5}$$

and the output randomness is given by the min-entropy function

$$R = -\log_2 P_{max} = -\log_2 \max_J \int_J^{J+\Delta} G\left(0, \frac{\gamma \sigma_t}{\gamma + 1}\right) \tag{6}$$

where J is the label of ADC bins, Δ is the resolution of ADC, $G(0, \sigma_t\sqrt{\gamma/(\gamma+1)})$ is a Gaussian distribution with zero mean and a variance of $\sigma_t^2\gamma/(\gamma+1)$, and $\int_J^{J+\Delta} G(0, \sigma_t\sqrt{\gamma/(\gamma+1)})$ is the probability to generate a certain sequence of random numbers. P_{max} is the maximum probability of some random number sequence occurs per sample, which can be calculated by the area under the probability density in an ADC bin. The conditional min-entropy of other type of QRNGs can be calculated with similar process.

Second, the bitwise XOR operation enhances the reliability of the random numbers in case some of the entropy sources are infiltrated by eavesdroppers. According to Shannon entropy theory[1], in Eq. (1), $Y(n)$ has the perfect secrecy to be all possible n-bit train, providing that any one of $X_i(n)$ is random and $X_i(n)$ trains are independent from each other. If only two trains $X_1(n)$ and $X_2(n)$ are applied, Eq. (1) is similar to the one-time pad, where $X_1(n)$, $X_2(n)$ and $Y(n)$ are corresponding to the key, the plaintext and the ciphertext respectively. Therefore, we do not need to trust all of the QRNGs but only at least one of them. As long as one of the QRNG entropy sources is reliable, the output $Y(n)$ is random. On the other hand, according to the Leftover Hash Lemma Eq. (3), the parameter ϵ characterizes the failure probability of the hashing function. Since the integrated QRNGs work independently, the total failure probability can be decreased by the XOR operation according to the union bound.

Third, depending on specific circumstances, different strategies can be applied to meet the requirements of different levels of security and speeds. For example, financial services such as Alipay require the utmost security. We need to close any possible loopholes in the cryptosystem. For this purpose, random numbers from various quantum devices are taken and processed as in Eq. (1). As a result, the highest speed is limited by the slowest QRNG at a rate of 16 Mbps. If end-users have concerns with some specific entropy sources or if any of the hardware breaks down, they can always choose an arbitrary combination of these QRNGs.

Finally, end-users are permitted to store and manage the random number files on the cloud. The generated random numbers could be used for encryption required by other services, either on the end-users' (e.g., Ant Financial) or remote-users' servers (e.g., Smart Access Gateway (SAG)). As those services are on the cloud, high-volume random numbers are required by thousands of servers and real-time post-processing is needed to meet the requirements of online encryption.

Practical implementation and applications

Our platform provides high-quality random numbers in a distributed network environment. The generated random numbers can be further combined with encryption protocols, such as Internet protocol security (IPsec) and SSL/TLS. In these protocols, the existing pseudo-random numbers used in key exchanges, authentication, and digital signatures are replaced with quantum random numbers. Pseudo-random numbers generated by deterministic algorithms will inevitably be predictable and reproducible. The quality of pseudo-random numbers is related to the complexity of the algorithm. With the increasing computing power, the security guaranteed by the complexity of the algorithm is seriously threatened. In contrast, QRNGs with intrinsic unpredictability can be used to greatly enhance the security of cryptosystems.

One example of the QRNG service for practical implementations is the SAG data encryption scenario. SAG is a cloud access solution for connecting hardware and software to the nearest Alibaba Cloud resources through the Internet in encrypted mode. SAG can connect branches (or outlets) and local data centers to the cloud, which enables enterprises to access the cloud more intelligently, safely and reliably. Since more than one million enterprise users from multiple industries are connected by SAG, secure access to the cloud is extremely important. The highly-random QRNG service can be used to enhance the security of the SAG, as shown in Fig. 4. The cloud QRNG transmits the highly-random numbers through RESTful (Representational State Transfer) or gRPC (google Remote Procedure Call) API through TLS to the Cloud Console,

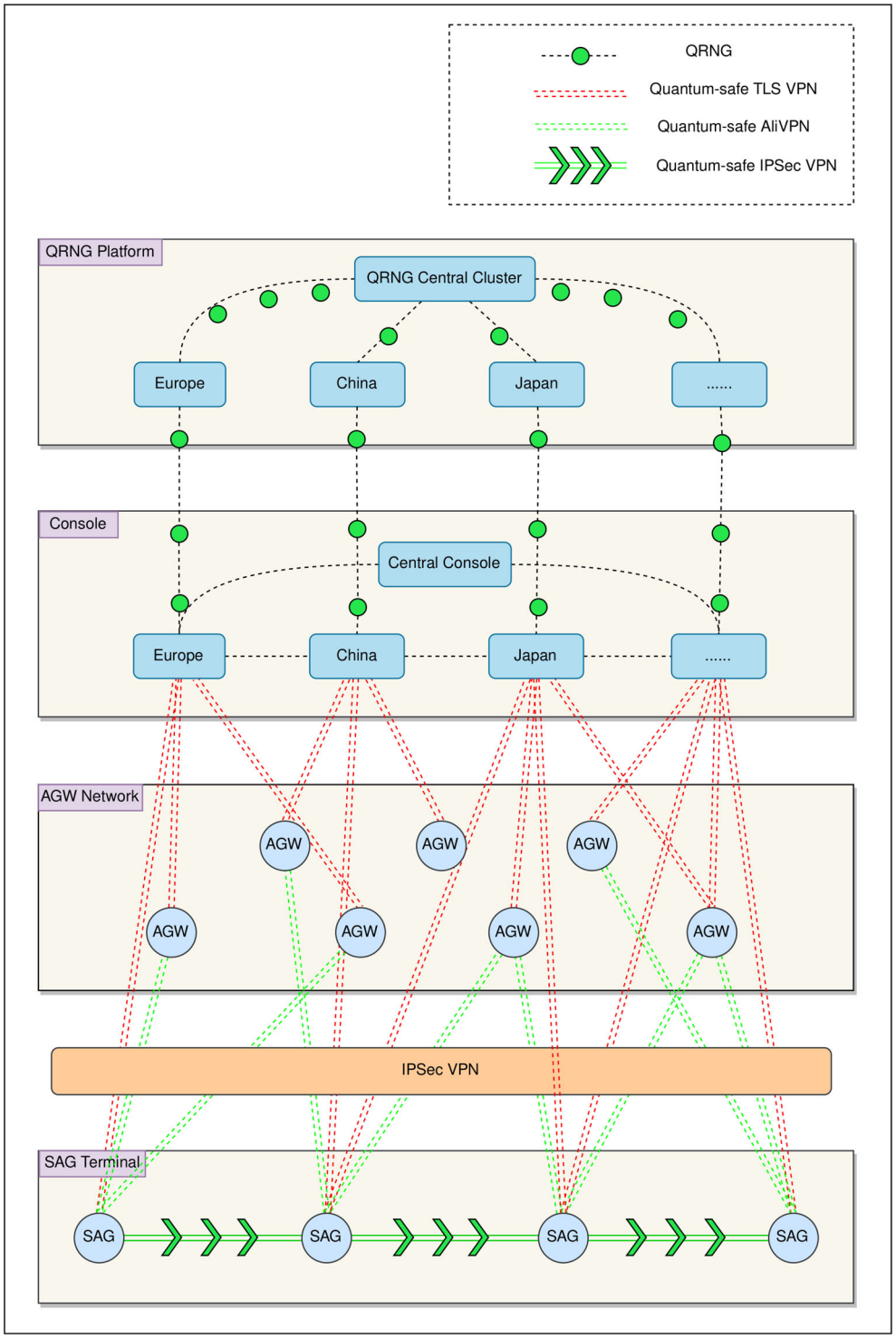

Fig. 3 QRNG in quantum-safe VPNs. Data flow of the generated random numbers from Alibaba QRNG Cloud Platform in the Smart Access Gateway.

which realizes unified monitoring and management of the overall network.

Another example is virtual private networks (VPNs). The QRNG platform is a practical step of implementations toward the full-process quantum-safe solutions in cloud services. The communication between SAGs and Alibaba Gateways can apply quantum-safe VPNs, whose architecture diagram is shown in Fig. 3. IPsec VPN based on StrongSwan is modified to be quantum-safe by implementing the techniques of quantum cryptography and post-quantum cryptography (PQC) algorithms. The mixed internet key exchange (IKEv2) in IPsec VPN can support three types of key exchange method: Diffie-Hellman, PQC algorithms, and quantum key distribution (QKD). It can dynamically update quantum PSK using QKD and replace the original pseudo-random numbers with quantum ones to enhance data encryption. Quantum-safe TLS VPN based on

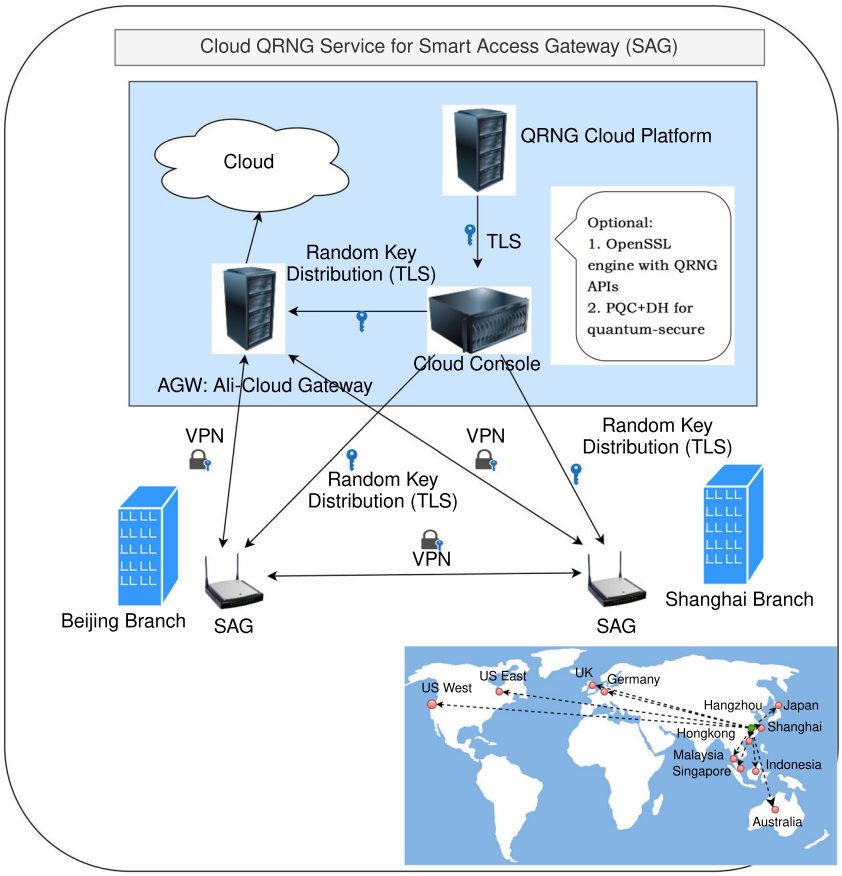

Fig. 4 QRNG service worldwide. Smart Access Gateway QRNG Cloud Implementation.

OpenSSL uses both Diffie-Hellman and PQC algorithms in the public key infrastructure (PKI) and the self-signed certificate authority (CA). The QRNG APIs is also integrated into an OpenSSL engine as a dynamic library in the TLS transmission, replacing all the random number modules inside the OpenSSL. A concrete example is AliVPN, which is a self-defined protocol for data encryption. Random numbers from the QRNG platform are used in AliVPN to enhance randomness of the keys. All the quantum-safe techniques are optional here in order to be compliant with security standards in some circumstances.

Similar implementations have also been demonstrated in Ant Financial, where the QRNGs are integrated into an OpenSSL engine as a dynamic library in data encryption of the Alipay cloud CA center. Quantum and pseudo-random numbers are switchable in the applications, which are compatible with current security standards. The generated random numbers are also distributed to end-users directly for certificate of authority and encryption in TLS protocols.

The QRNG service is worldwide, provided to ten different places at Shanghai, Japan, Hongkong, Singapore, Malaysia, Indonesia, Australia, United Kingdom, Germany, US East, US West, as shown in Fig. 4.

DISCUSSION

True random numbers are critical components in all cryptosystems. The major advantage of the QRNG platform over the other ones is it can avoid the loopholes of predictable random numbers. The motivation to reduce costs and increase robustness in quantum cryptography remains a great challenge, but the demonstrated feasibility of implementing quantum random numbers in cryptosystems represents an important step toward enhancing the security of classical communications using quantum technologies. The applications in SAG and Ant Financial show the practical implementation of quantum technology in data encryption. Our platform demonstrates quantum random number services with sufficient and adaptive generation speeds, reasonably low costs, controllable risks, high stability, and simple maintenance.

Our scheme shows the feasibility of providing high-quality random numbers in a distributed network environment. The random numbers generated by this scheme can be combined with encryption-related protocols (IPsec, SSL/TLS), identity authentication technologies, or key management systems. The cloud QRNG platform can also be accessed by different end-users in QKD systems, and the generated quantum random numbers can be used as seeds during the QKD communication.

Table 1. Quantum random number generation from different entropy sources.

No.	Type	Device	Speed	Interface
1	Single-photon Detection	IDQ Quantis-PCIe-16M	16 Mbps	PCIe
2	Phase-fluctuations	QuantumCTeck QRG-100E	300 Mbps	USB
3	Photon-counting	MPD-QRN-16	16 Mbps	USB
4	Vacuum-fluctuations	Lab-made QRNG prototype	400 Mbps	Ethernet
5	Hybrid	(1⊕2⊕3⊕4)	16 Mbps	–

Table 2. Random numbers from QRNG sources pass the NIST randomness tests.

Statistical test	Single-photon		Phase-noise		Photon-counting		Vacuum-noise		XOR	
	P-VAL	Prop.	P-VAL	Prop.	P-VAL	Prop.	P-VAL	Prop.	P-VAL	Prop.
Frequency	0.445	0.989	0.204	0.990	0.846	0.987	0.508	0.993	0.274	0.993
Block Frequency	0.581	0.986	0.406	0.992	0.465	0.994	0.375	0.988	0.871	0.990
Cumulative Sum	0.591	0.987	0.662	0.991	0.591	0.987	0.547	0.994	0.210	0.993
Runs	0.626	0.986	0.239	0.987	0.443	0.991	0.469	0.988	0.793	0.990
Longest Run	0.732	0.982	0.105	0.985	0.437	0.990	0.950	0.987	0.248	0.993
Rank	0.951	0.991	0.102	0.992	0.477	0.987	0.150	0.982	0.720	0.997
FFT	0.170	0.987	0.552	0.990	0.448	0.985	0.017	0.986	0.972	0.987
Non Overlapping	0.121	0.989	0.748	0.990	0.121	0.989	0.143	0.990	0.501	0.990
Overlapping Template	0.233	0.987	0.192	0.992	0.730	0.983	0.022	0.990	0.679	0.986
Universal	0.526	0.989	0.076	0.982	0.538	0.986	0.062	0.990	0.756	0.990
Approximate Entropy	0.820	0.991	0.098	0.990	0.380	0.987	0.625	0.987	0.265	0.995
RandomExcursions (RE)	0.975	0.987	0.980	0.986	0.975	0.987	0.846	0.990	0.100	0.988
RE Variant	0.585	0.987	0.548	0.991	0.585	0.987	0.530	0.990	0.532	0.991
Serial	0.584	0.989	0.050	0.988	0.584	0.989	0.269	0.995	0.722	0.989
Linear Complexity	0.028	0.995	0.115	0.984	0.023	0.990	0.827	0.990	0.087	0.993

For tests with multiple outcomes, a Kolmogorov–Smirnov (KS) uniformity test has been performed for p values (P-VAL), and the corresponding proportions (Prop.) are averaged.

For future work, we will consider applications with post-quantum algorithms and QKD, since the current distribution of random numbers using classical SSL/TLS is still an issue from the quantum-safe point of view. Integrated QRNG-chip embedded into the SAG devices is also under development to meet certain requirements. Finally, we will develop and integrate more different QRNGs to enhance the security and speed of the system.

METHODS

Performance of different entropy sources

The cloud-based high-performance QRNG platform is compatible with different types of QRNGs, whose randomness depends on various techniques. Different entropy sources can be chosen to generate the final random keys, which helps prevent from instability or randomness issues caused by individual QRNG device, and increases the reliability of the whole system. Online randomness testings have been performed regularly to ensure the quality of the entropy sources by taking advantages of the computing power on the cloud server. The unpredictability of quantum random numbers comes from the basic principles of quantum mechanics, which guarantees the security of encryption. End-users do not need to understand the underlying hardware equipment and related interfaces, and can simply obtain stable, high-speed, high-quality quantum random numbers for data encryption.

As mentioned earlier, the four different types of QRNGs connected to the platform are based on single-photon detection, photon-counting detection, phase-fluctuations, and vacuum-fluctuations with different interfaces and speeds. To ensure the reliability of the platform, a lab-made vacuum-fluctuation QRNG device is implemented together with three commercially available QRNG devices. The type of the single-photon detection QRNG is Quantis-PCIe-16M from ID Quantique, the type of the phase-fluctuation QRNG is QRG-100E from QuantumCTeck, and the type of the photon-counting QRNG is QRN-16 from Micro-Photon Devices. Table 1 shows the random number generators of different types, speeds and interfaces.

Standard randomness tests

Standard NIST randomness tests have been performed on the generated quantum random numbers at a size of 1 Gbit (1000 of 1 Mbit) from different sources and the test results are shown in Table 2. Note that hundreds of tests have been performed and Table 2 only shows one typical example of each devices. The test results (p values and proportions) vary for different sets of random numbers. It turns out that the randomness in most of the generated random number is sufficient to pass the NIST tests. The operation of XOR normally helps to improve values of P-VAL and Proportion, together with the decreasing of the total failure probability ϵ of the hashing function in Eq. (3).

DATA AVAILABILITY

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Received: 10 October 2020; Accepted: 18 May 2021;
Published online: 07 July 2021

REFERENCES

1. Shannon, C. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
2. Kerckhoffs, A. La cryptographie militaire. *des. Sci. Militaires* **IX**, 5–83 (1883).
3. Metropolis, N. & Ulam, S. The monte carlo method. *J. Am. Stat. Assoc.* **44**, 335–341 (1949).
4. Kelsey, J., Schneier, B., Wagner, D. & Hall, C. Cryptanalytic attacks on pseudorandom number generators. *Fast Softw. Encrypt.* **1372**, 168–188 (1998).
5. Guedes, E. B., de Assis, F. M. & Lula, B. Quantum attacks on pseudorandom generators. *Math. Struct. Comput. Sci.* **23**, 608–634 (2013).
6. Goldberg, I. & Wagner, D. Randomness and the netscape browser. *Dr. Dobb's J.* **21**, 66–70 (1996).
7. Ahmad, D. Two years of broken crypto: Debian's dress rehearsal for a global pki compromise. *IEEE Secur. Priv.* **6**, 70–73 (2008).
8. Heninger, N., Durumeric, Z., Wustrow, E. & Halderman, J. A. Mining your ps and qs: detection of widespread weak keys in network devices. In *Proceedings of the 21st USENIX Security*, 205–220 (USENIX, 2012).
9. KIM, S. & Han, D. Practical effect of the predictability of android openssl prng. *IEICE Trans. Fundament.* **E98.A**, 1806–1813 (2015).
10. Zheng, Y. Breaking real-world implementations of cryptosystems by manipulating their random number generation. In *Proceedings of SCIS 1997*, 6B1–6 (Springer LNCS, 1997).
11. Rarity, J. G., Owens, P. & Tapster, P. R. Quantum random-number generation and key sharing. *J. Mod. Opt.* **41**, 2435–2444 (1994).
12. Gennaro, R. Randomness in cryptography. *IEEE Secur. Priv.* **4**, 64–67 (2006).
13. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *Npj Quantum Inf.* **2**, 16021 (2016).

14. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89**, 015004 (2017).
15. Goldreich, O., Graham, R. L. & Korte, B. Modern Cryptography, Probabilistic Proofs, and Pseudorandomness. *ISBN* 3-540- 64766-x. Vol 17. (Springer-Verlag, 1998).
16. Soucarros, M., Canovas-Dumas, C., Clédière, J., Elbaz-Vincent, P. & Réal, D. Influence of the temperature on true random number generators. In *Proceedings of the IEEE HOST*, 24–27 (IEEE Xplore, 2011).
17. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **47**, 595–598 (2000).
18. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).
19. Dynes, J. F., Yuan, Z. L., Sharpe, A. W. & Shields, A. J. A high speed, postprocessing free, quantum random number generator. *Appl. Phys. Lett.* **93**, 031109 (2008).
20. Ma, H.-Q., Xie, Y. & Wu, L.-A. Random number generation based on the time of arrival of single photons. *Appl. Opt.* **44**, 7760–7763 (2005).
21. Wayne, M. A. & Kwiat, P. G. Low-bias high-speed quantum random number generator via shaped optical pulses. *Opt. Express* **18**, 9351–9357 (2010).
22. Wahl, M. et al. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Appl. Phys. Lett.* **98**, 171105 (2011).
23. Li, S., Wang, L., Wu, L.-A., Ma, H.-Q. & Zhai, G.-J. True random number generator based on discretized encoding of the time interval between photons. *J. Opt. Soc. Am. A* **30**, 124–127 (2013).
24. Nie, Y.-Q. et al. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Appl. Phys. Lett.* **104**, 051110 (2014).
25. Sanguinetti, B., Martin, A., Zbinden, H. & Gisin, N. Quantum random number generation on a mobile phone. *Phys. Rev. X* **4**, 031056 (2014).
26. Gabriel, C., Wittmann, C., Marquardt, C. & Leuchs, G. A generator for unique quantum random numbers based on vacuum states. *Nat. Photon.* **4**, 711–715 (2010).
27. Symul, T., Assad, S. M. & Lam, P. K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.* **98**, 231103 (2011).
28. Jofre, M. et al. True random numbers from amplified quantum vacuum. *Opt. Exp.* **19**, 20665–20672 (2011).
29. Haw, J. Y. et al. Maximization of extractable randomness in a quantum random-number generator. *Phys. Rev. Appl.* **3**, 054004 (2015).
30. Qi, B., Chi, Y.-M., Lo, H.-K. & Qian, L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt. Lett.* **35**, 312–314 (2010).
31. Xu, F. et al. Ultrafast quantum random number generation based on quantum phase fluctuations. *Opt. Exp.* **20**, 12366–12377 (2012).
32. Zhou, H., Yuan, X. & Ma, X. Randomness generation based on spontaneous emissions of lasers. *Phys. Rev. A* **91**, 062316 (2015).
33. Abellan, C. et al. Quantum entropy source on an inp photonic integrated circuit for random number generation. *Optica* **3**, 989–994 (2016).
34. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223 (2018).
35. Liu, Y. et al. Device-independent quantum random-number generation. *Nature* **562**, 548 (2018).
36. Cao, Z., Zhou, H., Yuan, X. & Ma, X. Source-independent quantum random number generation. *Phys. Rev. X* **6**, 011020 (2016).
37. Marangon, D. G., Vallone, G. & Villoresi, P. Source-device-independent ultrafast quantum random number generation. *Phys. Rev. Lett.* **118**, 060503 (2017).
38. Zhou, H., Zeng, P., Razavi, M. & Ma, X. Randomness quantification of coherent detection. *Phys. Rev. A* **98**, 042321 (2018).

ACKNOWLEDGEMENTS

We acknowledge helpful discussions with Zhongliang Sun and Yang Yang from Smart Access Gateway and Ant Financial department.

AUTHOR CONTRIBUTIONS

L.H. initialized the project. L.H. and H.Z. designed the protocol. K.F. wrote the code and assisted with the practical implementations. C.X. supervised the project. All authors contributed to discussing the results and writing the paper.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to L.H.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.