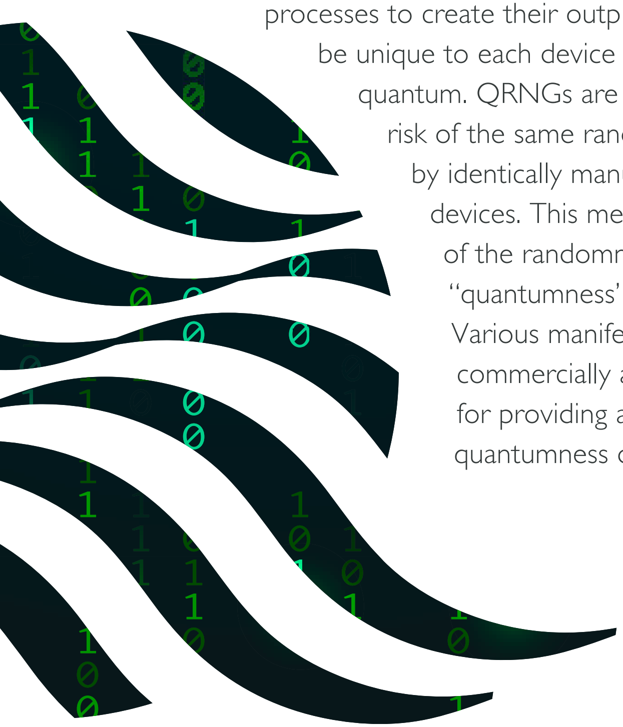
QUANTUM
COMMUNICATIONS
HUB

Quantum
Random Number Generators

Digital infrastructure permeates every sector and part of society. Cyber security is the protection of all this infrastructure – communications, remote connections, computing, IoT devices, etc. This security is built on cryptography and processes that consume random data, provided by random number generators (RNGs). Not only is it critical for the security that the consumed data be random, but also it is also essential that the data are unique. Different RNGs must not produce the same outputs, even if these are random. Whilst current tests for RNGs can assure randomness, these tests cannot assure output sequence uniqueness. There is currently no assurance that the random numbers generated are unique, and hence unpredictable, which potentially compromises security. Quantum Random Number Generators (QRNGs) offer a solution to this problem.

QRNGs are devices that utilise the inherent randomness of physical processes to create their outputs, assured by Nature to be unique to each device provided that the process is quantum. QRNGs are thus superior to RNGs, with no risk of the same random sequence being produced by identically manufactured and prepared QRNG devices. This means that assuring the uniqueness of the randomness requires assuring the "quantumness" of the process creating the data. Various manifestations of QRNGs are currently commercially available; however, a method for providing authoritative certification of their quantumness does not currently exist.



Work is ongoing in the Quantum Communications Hub to support the need for certification of QRNGs, to overcome this existing important technological barrier for the commercial and industrial exploitation of QRNGs. Hub researchers have established the principles for assuring the quantumness within current QRNGs, working closely with the UK's national metrology institution, the National Physical Laboratory (NPL), and various industrial partners. This work has underpinned a new Industrial Strategy Challenge Fund (ISCF) project – led by NPL – that will now establish the processes and standards needed to assure the unique randomness of QRNGs. Once these processes are in place, commercial QRNG products will be highly beneficial to UK telecommunications, defence, finance and banking industries, among others, as all such users can then be certain that the products are assured, accredited and trustworthy.

In addition to this assurance programme, Hub researchers are also working on more efficient and compact QRNGs, with new prototypes being developed. Next generation, so-called device-independent (DI) QRNGs are being brought closer to low-cost implementation, by assessing what is feasible with current and near-future technology and adapting protocols accordingly. DI-QRNGs have great potential for the future – these devices utilise quantum entanglement to hugely streamline their required assurance processes and standards. Such new, next-generation QRNGs, alongside other quantum security technologies based on entanglement, will offer an even broader spectrum of assured security solutions in the future.

If you would like to hear more about the Hub's work on QRNGs and their assurance, please contact us via enquiries@quantumcommshub.net

UK NATIONAL
QUANTUM
TECHNOLOGIES
PROGRAMME

UKRI

Engineering and
Physical Sciences
Research Council