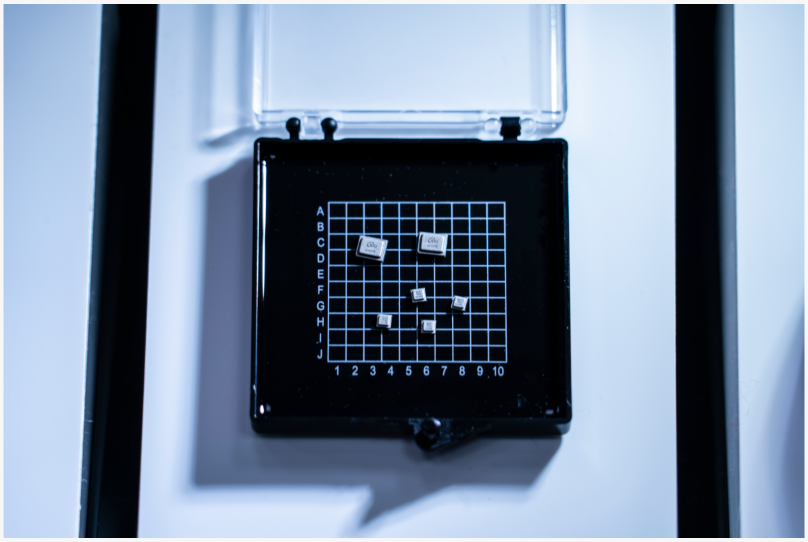
EINPRESSWIRE

Quantis QRNG Chip receives NIST Entropy Source Validation (ESV) Certification on IID Track

ID Quantique's range of QRNG chips are the first quantum-based RNGs to receive NIST Entropy Source Validation (ESV) Certification on IID Track.



ID Quantique's range of QRNG chips

OTTAWA, CANADA, September 20, 2023 /EINPresswire.com/ -- ID Quantique's range of Quantum Random Number Generator (QRNG) chips are the first quantum-based RNGs's to receive NIST Entropy Source Validation (ESV) Certification on IID Track.

Today at the International Cryptographic Module Conference (ICMC23), ID Quantique (IDQ) announced that its Quantis QRNG chips have just received NIST ESV certification on the Independent and Identically Distributed (IID) entropy estimation track. This certification offers the highest attainable security and robustness level for the generation of random bits. It makes IDQ's range of QRNG chips ideal for all security applications and integration into devices for automotive, computing, critical infrastructure, IoT, mobile and space communications to meet the most stringent security requirements.

> This certification is a major step for all users of our QRNG chips and QKD systems, as they will know that they can place increased trust in the use of these random numbers, yet at an affordable cost."
>
> *Gregoire Ribordy, CEO and co-founder of ID Quantique*

Historically, randomness was mainly used in the gaming industry. In the computer age, this was extended to modeling and simulations. Since the advent of the Internet, the need for cybersecurity applications has accelerated, to secure data in transit and at rest via encryption. Generating reliably high-quality randomness is a prerequisite for all cryptographic techniques. The increase of interconnected devices and exponentially growing volume of data generated and communicated makes cryptography ubiquitous, which in turn creates the need for small, reliable and high-quality randomness sources.

Various governments have set up cryptographic validation programs in order to allow users to assess the practical security of and gain confidence in their cryptographic systems. In the US, the National Institute of Standards (NIST) has developed the Cryptographic Module Validation Program (CMVP). Random number generation being so central to cryptography, the CMVP makes use of an entropy source that has been evaluated according to the NIST Entropy Source Validation (ESV) program a requirement. Since October 2022, it is for example mandatory for crypto modules aiming at FIPS 140-3 certification to have an ESV validated entropy source. Parties developing cryptographic solutions used by the US government will have to be certified according to the CMVP program of NIST and therefore use an ESV certified random number generator.

ID Quantique is proud to announce that its Quantis QRNG chips product range has just received ESV certification on the Independent and Identically Distributed (IID) entropy estimation track. NIST has verified that the random bits produced by the Quantis QRNG chips are independent and uniformly distributed. The independence property means that observing some bits does not provide any information on future bits to be generated. The uniform distribution property implies that 0's and 1's are equally likely to be generated. To obtain that high level of quality of entropy, IDQ's patented QRNG technology exploits the fact that the number of photons emitted by a common light source fluctuates randomly by nature. These fluctuations, also called "quantum shot noise", are purely of a quantum origin, and are therefore fundamentally random as per the laws of quantum physics and totally immune from environmental perturbations, resulting in a guaranteed reliable and stable source of entropy. This certificate provides the assurance that a particular entropy source conforms to NIST SP 800-90B and IDQ's QRNG chips fully meet these requirements.

ID Quantique is the first company to achieve an ESV certificate with a quantum-based entropy source and IID estimation track. Such quality of randomness provides the most trusted random keys for encryption techniques. IDQ has made use of the tests and qualification services of EWA Canada to achieve the world's first IID track Entropy Source Validation (ESV) (see Certificate #63). This certificate will also facilitate IDQ's customers certifications through the NIST's Cryptographic Module Validation Program (CMVP).

IDQ uses its Quantis chips in all its security products and solutions, such as its 4th generation of Quantum Key Distribution (QKD) range of solutions, the XG series, and its Key Management Solution Clarion KX.

"Security professionals are seeking the highest quality and most reliable source of entropy available, and they are right to do so. This certification is a major step for all the users of our Quantis chips and QKD systems, as they will know that they can place increased trust in the use of these random numbers, yet at an affordable cost. Entropy must not be a luxury product."

Grégoire Ribordy, CEO ID Quantique

Catherine Simondi
ID Quantique
+41 22 301 83 71
email us here
Visit us on social media:
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/656664274