

TROPOS

True Random numbers play an important role in data security to provide robust encryption. QRNG from QNu labs addresses different data rates and standard interfaces to cater to multiple applications.



TROPOS QNL - QRNG -X- 100G

— OVERVIEW

Traditional random number generators like PRNG and TRNG use predictable inputs which are deterministic. These inputs have a higher probability of repeating which creates predictability. Hence, making the entire system vulnerable.

Tropos quantum random number generator (QRNG) uses the principles of quantum mechanics to generate truly random numbers. In fact, quantum physics is fundamentally random in nature which has been confirmed by theory and experimental research.

Quantum Random Number Generator is a highly sophisticated engineering innovation that involves the power of complex deep-tech technologies (such as semi-conductors, opto-electronics, high precision electronics and quantum physics) working together to create the highest level of randomness possible.

— HOW QRNG WORKS

A laser-based quantum source generates the randomness in Tropos quantum random number generator.




To elaborate on the process, a laser produces a stream of elementary particles (photons). The photons generated from the laser are used to generate the random numbers.

These photons unlike classical objects are unpredictable under certain situations. When it is incident is on a semitransparent mirror, the photon has a 50/50 chance of being reflected or transmitted. The photon is then in a superposition of both the states (reflected and transmitted), i.e. the photon exists in both the states simultaneously. Upon measurement, it collapses to one of these states, which is intrinsically random and there is no way to predict which state the photon will collapse to. This gives the



inherent randomness from the photons, which cannot be influenced by any external parameters.

— **KEY TAKEAWAYS**

-  Perfect Random Keys
-  High Rate of Entropy
-  High Throughput Key Rates
-  Multiple Application Usage

— **USE CASES**

DEFENCE

Wireless Quantum Safe VPN

Wireless networks are on the rise, but this comes at the cost of security. The vulnerability increases many times when national security is involved. Though VPN (Virtual Private Network) is implemented in secure communications, randomness is not enough. We implement Tropos’s randomness to increase the security of encryption and Hodos (PQC) for post-quantum security. Quantum-Safe VPN covers Wi-Fi, Li-Fi, Ethernet and multipoint communications. The Quantum-Safe VPN can be implemented for indoor spaces like office and inter-building communications, along

with external spaces for inter-building and communication across different devices. Quantum-Safe VPN is an end-to-end communication tunnel between devices across various nodes of the network.

Identity Management

QRNG technology can be applied to ID card systems to generate random numbers every time an ID card is used and, subsequently, track every personnel movement (especially at defence facilities) to curtail unnecessary movement.

Quantum Secure Data Storage

Data needs to be stored without any lapses for vulnerabilities and latency. QNu aims to improve security by having a quantum layer that integrates with the present infrastructure and provides much-needed security. Tropos QRNG solves the problem of randomness.

Authentication and IAM

Digital certificates are very important for authentication and identity management. Certificates need random seeds for generating public and private keys. Hence, we integrate Tropos (QRNG) for better randomness and Hodos (PQC) for a higher level of security compared to RSA based certificates. In the case of classical certificates, which includes RSA and ECDSA, we replace the seed from which the key pair is derived. This increases the security many folds in authentication and IAM without any changes in the infrastructure.



Routing

Quantum Random Number Generator can be applied to the random routing of military weapons, equipments and supplies. Thereby, preventing enemies from pinning the locations of the used routes. This randomization of routing can be applied for land, air and water transportation routes between nodal points, as well as randomization of routes between the nodes.

Cryptography

The Quantum Random Number Generator is applied to generate keys for confidential transactions or top-secret messages, in addition to systems for launching operations (i.e. Command Centre) or missile launch systems.

Wireless Network for Security Monitoring

The secured wireless network will be utilised for the integration of IoT Sensors/ Wireless Cameras/ IR Sensors etc., for capturing data and transmitting it over the wireless network to a centralized monitoring location. Further, a secured wireless network will also provide mobility to sensor mounted vehicles as per requirement within the range of the directional antenna.

BANKING

Tokenization

Tokenization has been, is, and will be the go-to way to secure and mask important

PAN (Personal Account Number) data of the customer. The criticality of tokenization is known in the banking world but with the increase in digital adoption, the demand for tokens has surged. The demand in turn has resulted in repetition and increase in correlation in token generation which results in a secure token generation. Tropos addresses this randomness need in the tokenization process without impacting the way tokens are used today.

OTP

OTPs are very important for payments, banking, and many other user authentication applications. The current random number generators have a high correlation with OTP generation, which makes them the weak link in authentication. Generating OTP using Tropos guarantees the randomness and throughput required for demand of up to a million OTP per second.

EDUCATION

Exams and Certifications

Tropos can be used to generate unique values that are important for various academic purposes. Unique Certificate ID will decrease the fraud caused due to duplicate certificates as the ID is random and there is no way to guess the ID of each certificate.

To reduce the scope of duplication, each student is assigned a unique project ID.

It can also be used in university labs to randomly allocate test samples. This raises



the learners' chances of experimenting with non-duplicated samples, and encourages them to think independently.

CRYPTOGRAPHY

Today's digitally connected world requires higher levels of security to maintain the confidentiality of personal and institutional data. This is achieved by relying on cryptography, for which, one of the critical elements is the unpredictability of the encryption keys generated and used for securing data. Additionally, authentication applications like identity & access management also require a strong cryptographic foundation based on unique tokens to verify the user's or application's access to the secured data.

Tropos ensures the creation of truly random encryption keys and unique digital tokens for highly secure crypto operations for maintaining data security and confidentiality.

DATA CENTRE

Data centres act as the processing, storage, and recovery points of critical data for any organization. Therefore, they are also most prone to the wholesale theft of an organization's digital assets. QNu's solutions are built to ensure a high level of data security for data in transit and at rest in data centres.

IOT

In a hyper-connected world with billions of sensors generating hundreds of billions of data points requires unique identification of sensor data upon its storage in big

data platforms – Tropos provides the necessary uniqueness to identify each data point for subsequent processing and storage.

R & D

Sampling

The strength of sampling is in selecting random inputs. This can be applied in statistical analysis to select random samples to optimize the study of the hypothesis with a high degree of sample randomness. This approach is also applicable in randomizing test variables in R&D as it shortens the timeframe in selecting inputs.

QRNG can generate the inputs randomly and run tests at a higher speed. Though this is mainly used for black-box testing where the output is known, researchers, too, can apply it to know the responsible inputs.

AUTOMOTIVE

V2X (vehicle-to-everything) refers to a smart, holistic ecosystem where all vehicles and their surrounding infrastructure are interconnected.

QNu's quantum-safe security solutions are specifically designed to protect data in motion across V2X ecosystems from existing and emerging threats, as well as those posed by quantum computing.

TELECOMMUNICATIONS

Telecommunication networks underpin the communication, collaboration and



media channels that service millions of organisations and billions of individuals every day.

QNu's range of quantum-safe security solutions is designed to secure data in motion across telecommunication networks against existing and emerging threats. Our solutions enable carriers to guarantee security while offering an additional revenue stream – security as a service.

GAMING AND LOTTERIES

Online gaming and lotteries need to provide outstanding randomness quality to secure customer transactions. In games of chance, it must not be possible for a player to increase their probability to win by discovering a bias towards certain outcomes in the game.

Tropos has become the reference hardware random number generator for industries that require high security and regulatory compliance.

Q → NU

qnulabs.com

qnulabs.com/schedule-a-demo/



CIN: U72900KA2016PTC096629

DIPP: DIPP5607 dt 21/07/2017

MSME: KR03B0149274

DSCI: DSCI/AM/2018/08

NASSCOM: NSCM/2018/11/5396