id Quantique SA

21.09.2023 – 09:42 Uhr

ID Quantiques Sortiment an Quantum Random Number Generator (QRNG)-Chips sind die ersten quantenbasierten RNGs, die die NIST Entropy Source Validation (ESV)-Zertifizierung für den IID Track erhalten haben.

Ottawa, On (ots/PRNewswire) -

Heute gab ID Quantique (IDQ) auf der International Cryptographic Module-Konferenz (ICM23) bekannt, dass seine Quantis QRNG-Chips gerade die NIST ESV-Zertifizierung für den Independent and Identically Distributed (IID) Entropy Estimation Track erhalten haben. Diese Zertifizierung bietet die höchstmögliche Sicherheits- und Robustheitsstufe bei der Erzeugung von zufälligen Bits. Es macht das IDQ QRNG-Sortiment ideal für alle Sicherheitsapplikationen und die Integration in Geräte für die Automobilindustrie, Informatik, kritische Infrastruktur, IoT, Mobilkommunikation und Raumfahrtkommunikation, wo die strengsten Sicherheitsanforderungen erfüllt werden müssen.

Früher wurde die Zufälligkeit hauptsächlich in der Gaming-Branche verwendet. Im Computerzeitalter wurde dies auf Modellierung und Simulationen ausgeweitet. Seit dem Aufkommen des Internets hat sich der Bedarf an Cybersicherheitsanwendungen beschleunigt, um Daten während der Übertragung und im Ruhezustand mittels Verschlüsselung zu sichern. Für alle kryptografischen Techniken ist die Schaffung einer zuverlässigen, hochwertigen Zufallsrate eine Voraussetzung. Die Zunahme vernetzter Geräte und das exponentiell wachsende Datenvolumen, das generiert und kommuniziert wird, macht die Kryptographie allgegenwärtig, was wiederum den Bedarf an kleinen, zuverlässigen und hochwertigen Zufallsquellen schafft.

Verschiedene Regierungen haben kryptografische Validierungsprogramme eingerichtet, um es Benutzern zu ermöglichen, die praktische Sicherheit ihrer kryptografischen Systeme zu bewerten und Vertrauen in sie zu gewinnen. In den USA hat das National Institute of Standards (NIST) das Cryptographic Module Validation Program (Validierungsprogramm für kryptografische Module, CMVP) entwickelt. Die Erzeugung zufälliger Zahlen ist so zentral für die Kryptographie, dass das CMVP die Verwendung einer nach dem NIST Entropy Source Validation (ESV)-Programm bewerteten Entropiequelle vorschreibt. Seit Oktober 2022 ist es beispielsweise obligatorisch für Kryptomodule, die eine FIPS 140-3-Zertifizierung anstreben, eine ESV-validierte Entropiequelle zu besitzen. Entwickler von kryptografischen Lösungen, die von der US-Regierung verwendet werden, müssen nach dem CMVP NIST-Programm zertifiziert werden und daher einen ESV-zertifizierten Zufallsnummerngenerator verwenden.

ID Quantique freut sich bekanntgeben zu können, dass seine Quantis QRNG-Chips-Produktreihe gerade die ESV-Zertifizierung für den Independent and Identically Distributed (IID) Entropy Estimation Track erhalten hat. NIST hat verifiziert, dass die von den Quantis QRNG-Chips produzierten Zufallsbits unabhängig und einheitlich verteilt sind. Die Unabhängigkeitseigenschaft bedeutet, dass die Beobachtung einiger Bits keine Informationen über zukünftige zu generierende Bits liefert. Die einheitliche Verteilungseigenschaft impliziert, dass 0 und 1 gleichermaßen wahrscheinlich generiert werden. Um dieses hohe Maß an Entropie zu erreichen, nutzt die patentierte QRNG-Technologie von IDQ die Tatsache, dass die Anzahl der von einer gewöhnlichen Lichtquelle emittierten Photonen von Natur aus schwankt. Diese Schwankungen, auch Quantenschussgeräusche genannt, sind rein quantenbedingt und daher nach den Gesetzen der Quantenphysik grundsätzlich zufällig und völlig immun gegen Umweltstörungen, was zu einer garantierten zuverlässigen und stabilen Entropie führt. Dieses Zertifikat gibt die Sicherheit, dass eine bestimmte Entropiequelle mit NIST SP 800-90B konform ist und die QRNG-Chips von IDQ diese Anforderungen vollständig erfüllen.

ID Quantique ist das erste Unternehmen, das ein ESV-Zertifikat mit einer quantenbasierten Entropiequelle und IID Estimation Track erhält. Eine solche Zufallsqualität bietet die vertrauenswürdigsten Zufallsschlüssel für Verschlüsselungstechniken. IDQ hat die Tests und Qualifizierungsdienste von EWA Kanada genutzt, um die weltweit erste IID Track Entropy Source Validation (ESV) zu erlangen (siehe Zertifikat Nr. 63). Dieses Zertifikat wird auch die Zertifizierungen der Kunden von IDQ durch das Cryptographic Module Validation Program (CMVP) von NIST erleichtern.

IDQ verwendet seine Quantis-Chips in all seinen Sicherheitsprodukten und -Lösungen, wie z. B. in der vierten Generation der Quantum Key Distribution (QKD)-Lösungen, der XG -Serie und der Schlüsselmanagementlösung

Clarion KX.

Für weitere Details wenden Sie sich bitte an:

Catherine Simondi

VP Marketing and Communication, ID Quantique Catherine.simondi@idquantique.com oder

+ 42 22 801 83 71

Foto – https://mma.prnewswire.com/media/2216480/QRNG_chips.jpg

Logo – https://mma.prnewswire.com/media/2089811/4286168/IDQ_Logo.jpg

View original content:https://www.prnewswire.com/de/pressemitteilungen/id-quantiques-sortiment-an-quantum-random-number-generator-qrng-chips-sind-die-ersten-quantenbasierten-rngs-die-die-nist-entropy-source-validation-esv-zertifizierung-fur-den-iid-track-erhalten-haben-301934455.html