重新定義何謂亂數

QUANTIS PCIe-40M & PCIe-240M

WHEN RANDOM NUMBERS CANNOT BE LEFT TO CHANCE

自2001年以來，Quantis QRNG產品已被廣泛做為各項應用中可信任的亂數來源，生成高品質的金鑰提供給加密模組，有效地保護存取私人網路、伺服器、虛擬機器和應用程式安全；確保資料的正確與機密性。其他應用包含遊戲產業、科學模擬或建模。

Provably secure

Quantis QRNG系列產品利用物理的量子光學運行概念，從本質上概率產生真亂數，基於量子光學概念是QRNGs被廣為認知的特點，可以清楚地建模與控制從第一個位元就能產生最高熵。然而可以簡易使用是ID Quantique旗下量子亂數產生器(QRNGs)的一大特點。

Quantis PCIe-40M和PCIe-240M內建IDQ20MC1晶片採用IDQ最新的QRNG技術，運作原理是透過 LED照射CMOS，然後透過讀取CMOS 產生的光源雜訊來隨機生成亂數序列。可直接從熵源(entropy data mode)生成隨機位元(bits) 或在符合NIST的後處理(RNG data mode)。即時狀態驗證與熵源健康狀態偵測能在晶片端確保PCIe總是提供最高熵，而且任何錯誤或攻擊發生都能立即偵測。

Compliant and certified

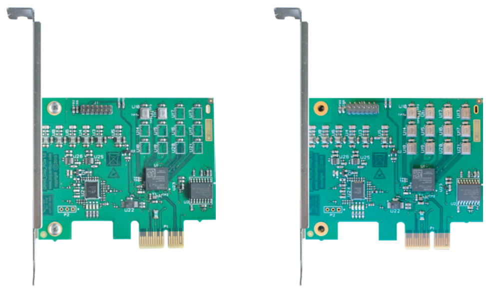
Quantis PCIe-40M和PCIe-240M皆符合NIST SP800 90A/B/C標準，通過IID, non-IID tests, DieHarder和NIST SP800-22測試套件。METAS和CC認證正在申請中。上一代 Quantis PCIe and USB也具備AIS31版本，符合德國BSI的AIS31認證。

實際應用產業

- 機敏資料的正確性及安全性
- AI（機器學習、深度學習）
- 保護終端客戶的設備、機器與網路
- 科學建模與模擬
- 金融交易傳輸/區塊鏈
- 遊戲、博奕產業

為什麼需要Quantis QRNGs?

- 可驗證的安全熵來源
- 從第一個位元就是真亂數
- 由量子光學本質上產生亂數
- 科學建模與模擬符合NIST後處理
- 即時狀態驗證與熵源健康狀態偵測
- 可整合至大多數作業系統



型號	PCIe-40M	PCIe-240M
效能		
Quantum entropy source	38.3 Mbps ± 5%	232 Mbps ± 5%
RNG Data Output (embedded NIST compliant DRBG)	9.6 Mbps ± 5%	58 Mbps ± 5%
Live status verification & entropy source health monitoring	✓	✓
認證		
NIST SP800-90A/B/C, SP800-22 and DieHarder test suite compliance	✓	✓
METAS Certification	pending	pending
BSI Common Criteria & AIS 31 certification	pending	pending
環境		
Thermal noise contribution	<1% (fraction of random bits arising from thermal noise)	
Storage temperature	-40 °C to +85 °C	-40 °C to +85 °C
Operating temperature	0 °C to +50 °C	0 °C to +50 °C
尺寸、介面		
Dimensions (mm)	80 x 63.75	80 x 63.75
Specification	PCI Express Base 1.0a compliant	
支援作業系統 **(QUANTIS LIBRARY AND EASYQUANTIS APPLICATION)***		
Windows 10	✓	✓
Ubuntu 18.04	✓	✓
CentOS 7	✓	✓

(*) Quantis library enables the production of random binary data, integers and floating point numbers. It can be used to access multiple Quantis generators and includes advanced functionalities such as random data scaling. The Quantis extensions libraries implement a randomness extractor which can be used to postprocess the output of the Quantis QRNG. Easy Quantis application allow to read and display random numbers or store them in a file.

RichSmart Technology Co., Ltd.
代理商 瑞奇數碼股份有限公司
台北市內湖區港華街66號1樓
TEL 02-26581786 | www.richsmt.com