重新定義何謂亂數

QUANTIS 真亂數產生器

WHEN RANDOM NUMBERS CANNOT BE LEFT TO CHANCE

雖然亂數在許多應用上都被採用，但其生成的方式常常被忽略。然而，透過電腦無法產出真亂數。既然量子物理學本質上就是隨機的，自然可以利用它作為隨機來源。Quantis是實體的亂數產生器，採用基本量子光學過程。光子-光粒子，一個一個被發送到半透明鏡面上同時進行偵測，被反射或穿透的結果產生對應0或1的值。

相較於常用的亂數來源，IDQ量子亂數產生器，具備不受環境干擾影響，並可以進行實際狀態驗證的優勢。Quantis實際運行時，會隨時進行監控，若有偵測到錯誤，該亂數位元流(bit stream)會立即被捨棄。再者，Quantis從第一個光子(bit)開始立刻提供完全亂數。Quantis具備USB介面，能輕易地整合至既有應用中。大部分常見的系統都能採用，具備API函式庫能簡易的存取並演示應用。

Quantis軟體中提供的進階功能，如scaling和randomness extraction可最大程度的擴充其應用範圍。

Quantis USB

產業應用

- 密碼學
- 樂透、線上遊戲
- PIN碼產生
- 數值模擬
- 統計研究
- 行動預付系統
- 安全列印

產品優勢

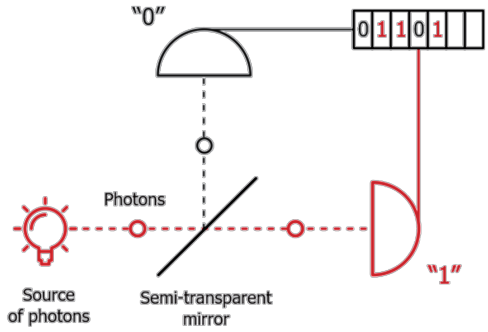
- 真量子亂數產生
- 經驗證之量子RNG技術
- 產生亂數速率高達4M bits/s
- 可提供Randomness extraction
- 持續狀態檢測
- 低成本
- 體積小可信賴
- 輕易整合至實際應用
- 快速產生亂數

Quantis的簡單概念同時也是他的優勢，由於量子力學的理論與運作模式已經廣為人知並易於表徵，對此產品的認證相對簡易。Quantis已獲得業界常用的真亂數認證，包含以下：

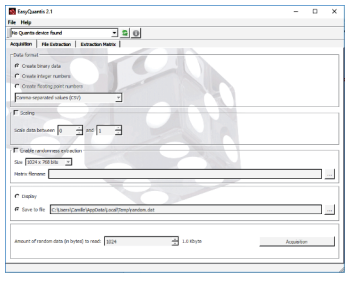
- NIST SP800-22 Test Suite Compliance
- METAS Certification
- CTL Certification
- Several iTech Labs individual Certificates
- Compliance with the BSI’s AIS31 standard (dedicated version of Quantis)

Quantis原理

基於量子的原理架構：
光子-光粒子，一個一個被發送到半透明鏡面上同時進行偵測，被反射或穿透的結果產生對應0或1的值。



QUANTIS 套裝軟體--EasyQuantis



Quantis搭配EasyQuantis軟體可讀取亂數並儲存於檔案中。可以下列格式產生：
■ Binary (二進位) ■ Integers (整數) ■ Floating point (浮點數)

EasyQuantis Application具備進階功能，如scaling和randomness extraction可最大程度的擴充其應用範圍。命令列(Command Line)介面也可用於存取Quantis並整合EasyQuantis於腳本(scripts)中。

Quantis函式庫

Quantis函式庫可用來存取Quantis QRNG(量子亂數)， API函式庫和USB函式庫非常相似能夠支援大多數系統。此函式庫能夠產生不同格式的亂數，如二進位、整數和浮點數。亦可用來存取多台Quantis亂數產生器並且能進行進階的功能如random data scaling。QuantisExtensions函式庫具備隨機擷取功能，可用來處理Quantis QRNG的產出亂數。

允許存取Quantis函式庫與樣本source code，支援下列程式語言：
■ C++ ■ C# ■ Java ■ VB.NET
Quantis也支援standard C++11 random device API

產品型號與規格

	 Quantis-USB-4M
亂數產生率[1]	4 Mbit/s ± 10%
熱雜訊Thermal noise contribution	< 1% (Fraction of random bits arising from thermal noise)
存放溫度	- 25 to + 85°C
尺寸	61 mm x 31 mm x 114 mm
搭配設備需求	需具備USB插槽
USB規格	2.0
支援作業系統	**V18.03.08** Windows 7, 8, (32位元. 64位元) Windows Server 2008, 2012, 2016 (32位元. 64位元) Free BSD Linux 2.6, 3.x, 4.x Mac OS X **V20.2.3** Windows 10 Ubuntu 18.04 Cent OS7

※1 : Hardware bit rate prior to randomness extraction

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