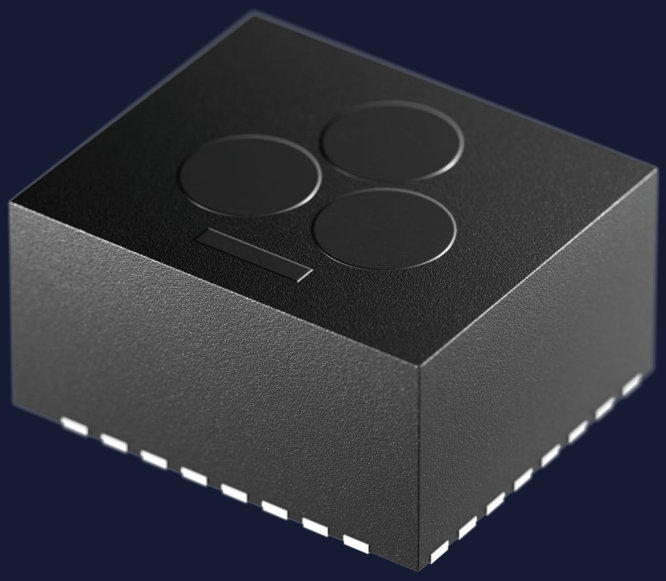
Quside

Product Datasheet

Quside Ruby™ S1



The Quside Ruby™ S1 is a Quside's proprietary quantum noise source, designed as the most compact and highly scalable solution within our products line. Based on VCSEL technology and able to generate up to 50 Mb/s of raw data.

Applications

The Quside Ruby™ S1 has been developed to be integrated into any system that can provide or require high-quality random numbers. The main applications for those kinds of systems are the following:

Transportation
• Software Defined vehicles hardware integration
• Security by design
• Enhanced security in-vehicle communications
• Future-proof deployments

Edge Computing
• Security foundation of the same level as in the datacenter
• Quantum-safe communications with the fog and the core computing networks
• Crypto-agility for future-proof deployments
• Efficient size and power consumption

Smart Industries
• Capillarity in the security foundations for the smart devices
• Reduced attack surface
• Crypto-agility for long-life devices

OT equipment manufacturers
• Suitable for low resources equipment
• Enhanced security for remote locations
• Future-proof with crypto-agility for ultra long live equipment

The Quside Ruby™ S1 is designed for high-performance quantum random generation for a broad range of target computing devices.

Features

Targeted performance
• 50 Mb/s raw generation rates

Unique connectivity
• Delivered in a 5-pin package, compatible with a variety of PCB designs.
• Designed for technology integrators.

Randomness quality
• Unconditional Min-entropy above 94%, and up to 99%.

Modular solutions
• With a careful design one or more chips could be integrated in the same PCB.

Performance self-verification
• Delivers a series of functionalities for metrology and monitoring of the entropy source and entropy quality

SPECIFICATIONS

	Units	Min	Typ	Max
VCSEL forward voltage	V	0	2	3
VCSEL operating current	mA	0	1	5
Modulation current	mA	2	-	6
PD reverse bias voltage	V	0	-3.3	-10
PD photocurrent	uA	40	100	400
Power consumption	mW	-	2	-
Operating speed	Mbps	-	50	-
Package bandwidth	MHz	-	-	500
Quantum to classical noise ratio (fclk = 500 MHz, T = 25°C)	dB	10	-	13

RAMDOMNESS SPECIFICATIONS

	Units	Min	Typ	Max
Unconditional min-entropy[1]	Bits	0.94	-	1
Raw bit rate	Mbps		50	
Running Average		0.48	-	0.52
Extracted bit rate[2]	Mbps		34.375	

[1] Min-entropy $H_{min} = -log_2(\max(p_i))$, with p_i the probability for 0 and 1, extracted directly from the random bits running average..
[2] Extraction rate of 0.688, using the randomness extractor from [D. Frauchiger, R. Renner, & M. Troyer (2013), arXiv:1311.4547].

ABSOLUTE MAXIMUM RATINGS

	Units	Min	Typ	Max
Bias monitor	mA	0.25	-	2.2
Monitored Operating Temperature (approx. 15°C above Env. Temperature)	°C	35	40	55
Environmental Operating Temperature[3]	°C	20	25	40
Storage Temperature	°C	10	-	80

THEORY OF OPERATION

Vertical cavity surface emitting lasers (VCSELs) emit laser light vertically from the surface of the semiconductor chip and are ideal for high-speed optical data transmission due to their physical properties. VCSELs can emit in two possible polarization modes, determined randomly when the laser is turned on.

QUSIDE exploits this property to generate quantum randomness by operating a VCSEL in a gain switching (GS) regime at a frequency of 10 - 50 MHz, causing the laser to repeatedly switch on and off, randomly selecting a polarization mode each time (see Figure 2 for more details). A polarization filter at the optical output allows only one mode to pass, which is then detected by a photodetector (PD). This results in a train of pulses with randomly determined polarization modes, as illustrated in Figure 2.

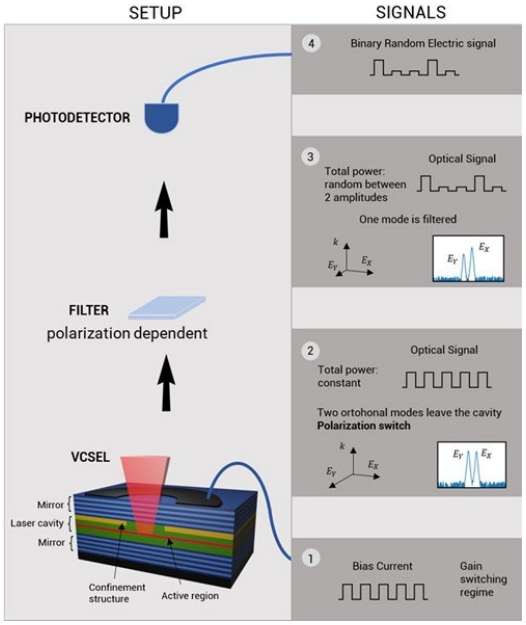


Figure 1: Description of the QRNG based on the VCSEL

[3] QRNG tested under the presented range: 20 – 40°C.

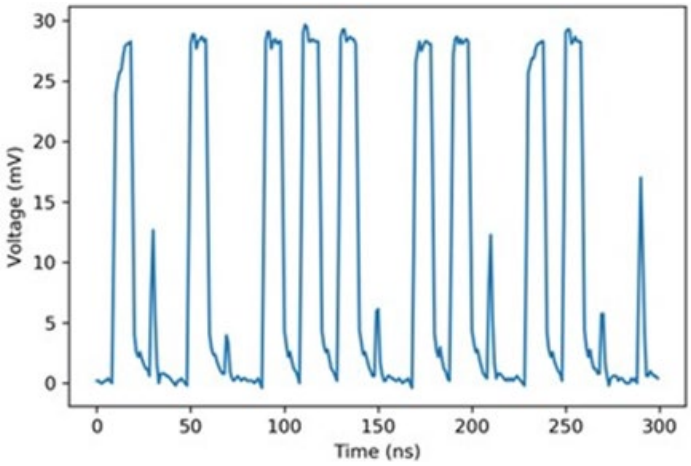


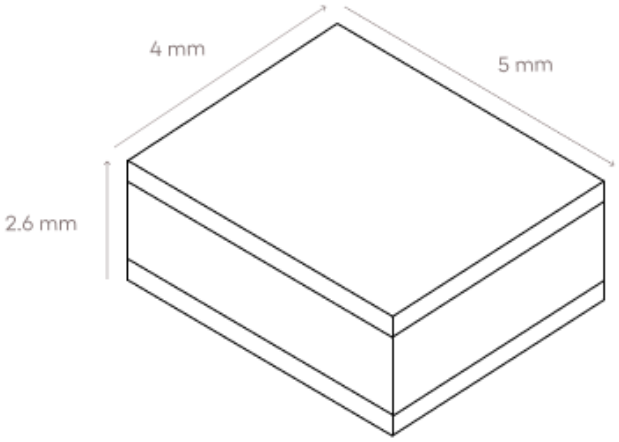
Figure 2: VCSEL random amplitude signal

PIN#	Mnemonic	Description
1	PD Cathode	Photodetector Cathode
2	VCSEL Anode	VCSEL Anode
3	VCSEL Cathode	VCSEL Cathode
4		
5	PD Anode	Photodetector Anode

MECHANICAL AND PIN OUT SPECIFICATION

The specifications of the packaged chip are shown in the tables below.

	Symbol	Units	Min	Typ	Max
Package area	A	mm		5x4	
Total number pins	N			5	
Connected pins				5	



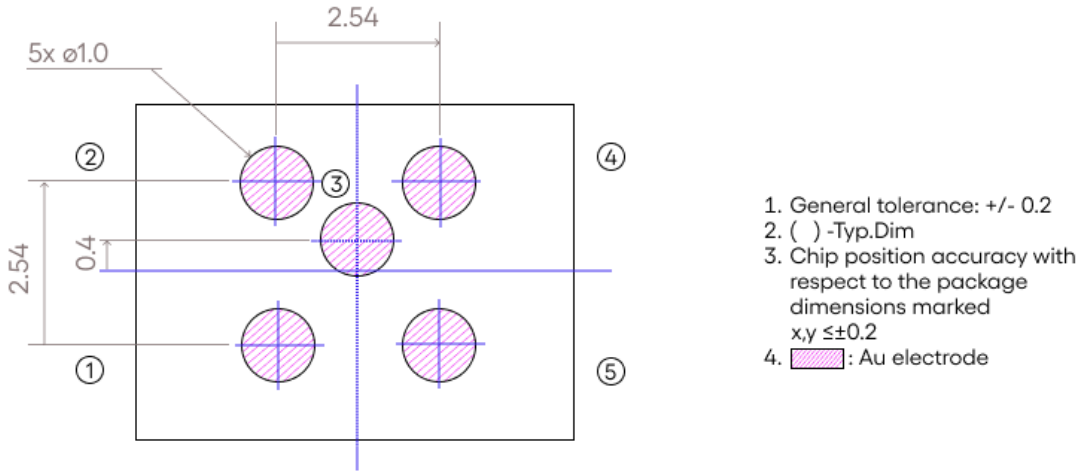


Figure 3 & 4: Quside Ruby™ S1 package pin

Thanks for being part of our quantum journey!

To learn more about our products visit
www.quside.com and contact: sales@quside.com

support@quside.com