IDQ6MC1 Chip Specification

QUANTUM RANDOM NUMBER GENERATOR

ID QUANTIQUE

Version : v2.6
Date : 2024-01-22

Distribution : Confidential

Document Revision History

VERSION	Date	COMMENT
1.0	2018-07-27	Describes the basic features of SKT's QRNG chip
1.1	2019-04-12	Figure 3-1, 3-2: Change signal name - VDD_IN ➔ VA, VST_INFO ➔ VI Table1 : add VI default value description
1.2	2019-06-19	Figure20. SDI input hold time. Table9 : add SDI input hold time value
1.3	2019-09-30	Status check command description 0x4100 ➔ 0x41 Figure-7: Change No Burst and 1-Burst figure Figure-16 modification Table9 : SPI interface timing value modification Figure 25~29 index repair Main Feature RNG/Sample Throughput - RNG : 1.5Mbps ➔ 1.47Mbps - Sample Noise : 6Mbps ➔ 5.88Mbps
1.93	2020-04-06	CSC ➔ SCS signal name exchange Figure 19~21. CSC signal name exchange to SCS
2.0	2020-03-31	S2q100 -> IDQ6MC1
2.1	2020-07-29	Correct error Sentences
2.2	2021-06-30	Specify confidential distribution and others minor aesthetics changes in headers and footers
2.3	2022-07-11	Remove the "3.2 IDQ6MC1 Operation Modes" section.
2.4	2022-07-25	Remove the "2.3 Connection for Unused Pins" section.
2.5	2023-01-12	Remove the "4.6 Information about sleep mode"
2.6	2024-01-22	Correct typos.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

Contents

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

List of Tables

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

List of Figures

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

IDQ6MC1 QRNG(Quantum Random Number Generator) Device

1. Device Overview.

1.1 Main Features

- **QRNG Core**
  - Compliant to the standard NIST 800-90A/B/C
  - 1.47Mbps RNG Data Output
  - 5.88Mbps Sample Noise Data Output
- **Power Supply Information**
  - 2.8V Single Input Voltage
    (Embedded two LDO Circuits for Digital & I/O Core)
  - Digital Core Voltage : 1.5V
  - Analog Core Voltage : 2.8V
  - I/O Interface Voltage : 1.8V
- **Power Consumption**
  - Generation RNG Code : 59.94mW
  - Sample Noise Output Mode : 58.24mW
- **Operation Frequency Clock**
  - Embedded ROSC : 41MHz~58MHz (Typ.: 48MHz)
  - Pixel & Analog Operation : 6MHz
  - I²C Interface Max Operation Speed : 100KHz
  - SPI Interface Max Operation Speed : 24MHz
  - Internal MCU Operation : 6MHz
- **Temperature Range**
  - Recommended Temperature: -30℃ to 85℃
  - Absolute Maximum Rated Temperature: -40℃ to 105℃
  - Storage Temperature: -40℃ to 125℃
  - AEC-Q100 qualified.
- **Memories (RNG/System)**
  - 14Kbyte MCU Code ROM
  - 1Kbyte MCU Data SRAM
  - 7Kbyte QRNG Output Buffer SRAM
- **Serial Communication**
  - SPI Interface for RNG & Sample Noise Data (selectable)
  - I²C Interface only for RNG Data
- **Package Dimension and Type**
  - 4.2 x 5.0 x 1.1mm
  - 14-Ball BGA Package Type
- **System Control Core**
  - TI MSP430™ Open Core
  - 16bit-RISC Processor
- **Embedded Analog Feature**
  - 2.8V to 1.8V Voltage LDO Circuit for I/O Supply
  - 2.8V to 1.5V Voltage LDO Circuit for Digital Core Supply
  - Analog POR (Power On Reset) Circuit
  - 2EA LED Current Driver Control Circuit
  - Analog ROSC (Ring Oscillator) Circuit for Main Clock Generation
  - Analog Over/Under Voltage Detection Circuit
  - 10-bit Serial Type ADC & CDS Circuit
- **Pixel Resolution & Frame Rate**
  - Active Resolution : 128x100
  - Total Pixel Resolution : 144x116
  - Optical Black Pixel : 4-Line
  - Frame Rate : 241fps
- **Pixel Information**
  - 3.0 x 3.0um Pixel Dimension
  - Conversion Gain : 160uV
  - FWC : > 8000e-
  - Dark Current : < 10mV/s @ 60℃

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

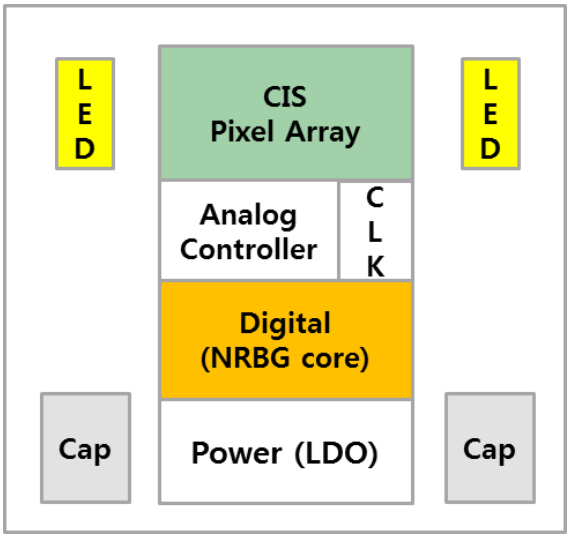
1.2. Applications

- Security-related Areas
  - All conventional cryptographic algorithms/protocols, functions, applications and services
  - Computing Device (mobile phone, Tablet, PC, Server, etc)
  - Automotive (V2X, CAN, Infotainment, etc)
  - Smart Network (IoT, LTE, WiFi, Smartgrid, SmartCity, SmartHome, etc)
- Non-security Areas
  - Scientific modeling and simulation
  - AI (Machine/Deep learning)
  - Game & Gambling

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

1.3. Basic Concepts

Our Quantum Random Number Generator (QRNG) chip provides an extremely high quality of randomness with the integrity and transparency of its operation. As an entropy source, the QRNG chip takes advantage of quantum shot noise. To observe(monitor) the quantum shot noise, various light sources are utilized, where coherent laser, thermal light, light emission diode (LED), etc. are good candidates. Since our main object is to make QRNG as a chip, we chose the LED technology as a light source and the CMOS image sensor (CIS) technology to detect and digitalize the intensity of a light source. Also, we integrated several digital core logics to distill a true random bit sequence from the quantum shot noise and control LEDs, CIS, core logic and interfaces. Both CIS and the digital logic are placed together on a single wafer by using the ASIC (application-specific integrated circuit) technology. The following figure shows a basic conceptual architecture of our QRNG chip.



The analog controller inside the chip plays a very important role as it automatically sets the brightness detected by pixels in a normal range, not too high and low in order to provide a good quality of entropy. It is done by controlling the amount of current applied to the LED and the exposure time of the CIS. Since the quantum shot noise of a light follows the Poisson statistical distribution (the mean value and the variance are equal), the brighter a light is, the higher entropy we can get. However, due to the limit of the input range of an analog-digital-converter inside the CIS, the detected brightness has to be set to avoid the saturation to the maximum value, and trivially the minimum value as well.

In addition, we would like to emphasize that our QRNG chip is more than just an entropy source, but a stand-alone true RNG. It follows a construction method of non-deterministic RBG mechanism of full-entropy with compliance to NIST SP800-B/C, which requires additionally proceeding with a deterministic RBG mechanism approved by FIPS 140-2 and reseeding it with a new entropy input right after generating a random bit string of full entropy.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

1.4. Functional Block Diagram

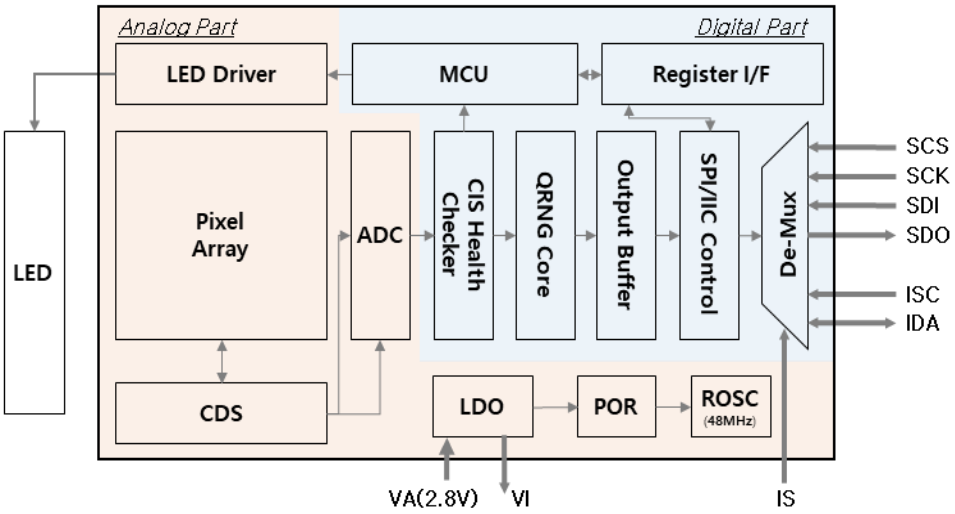


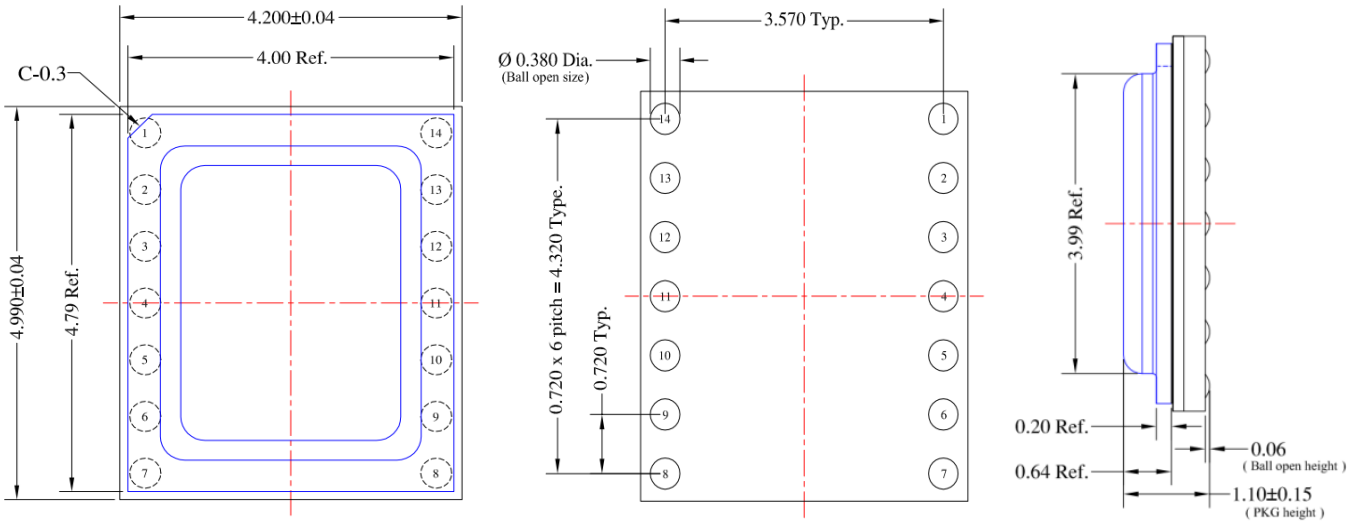
Figure 1. IDQ6MC1 Function Block Diagram

IDQ6MC1 is a Quantum Random Number Generation (QRNG) chip based on a CIS sensor. The LED is built in the chip as an entropy source and a CIS sensor digitalizes the amount of entropy. IDQ6MC1 supports two serial interfaces SPI and I²C, which can be chosen by the IS pin configuration. In addition, it also embeds an open core, called MSP430 (MCU) to control all analog and digital blocks. Two internal LDOs are used for 1.5V and 1.8V power supply respectively and OVD (Over Voltage Detection) and UVD (Under Voltage Detection) functions are built-in to detect the abnormal voltage input. The CIS has 128x100 active pixel resolution and the internal ADC that converts the charged voltage in each pixel to 10-bit digital value. As a stand-alone chip, it also owns its internal POR (Power On Reset) and ROSC (Ring Oscillator) circuits.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

2. IDQ6MC1 Pin Configuration & Package Information

2.1. IDQ6MC1 Package Dimension



(a) Top View **(b) Bottom View** **(c) Side View**

Figure 2. IDQ6MC1 BGA Package Dimension Information

2.2. IDQ6MC1 Pin Descriptions

Table 1. IDQ6MC1 Pin Description

FUNCTION	PIN NAME	PIN NO	PIN TYPE	Description
Power	VA	2	-	2.8V Power Supply
	VS	13	-	Ground Supply
I²C	ISC	4	I	I²C Serial Clock Input (IS PIN = High)
	IDA	5	I/O	I²C Serial Data In/Out (IS PIN = High)
SPI	SCK	3	I	SPI Slave Mode : SPI Chip Selection Input - IS = '0' & ISC = '1' SCK (SPI Serial Clock), SDO (SPI Serial Data Out) SDI (SPI Serial Data In), SCS (SPI Chip Enable)
	SDO	9	O	
	SDI	6	1	
	SCS	11	I	
IF Selection	IS	10	I	I²C & SPI Protocol Selection - High('1') = I²C Protocol, Low('0') = SPI Protocol
Monitoring	VI	12	O	Input Supply Voltage Status Monitor Pin - 2.38V ~ 3.22V : High (Stable Input Voltage Range) - > 3.22V : Low Output (Over Voltage Detection) - < 2.38V : Low Output (Under Voltage Detection) - Default : High (1.8V)
NC	NC	1,7,8,14	NC	NC

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

3. Chip Implementations

3.1. IDQ6MC1 Voltage Status Check (VI)

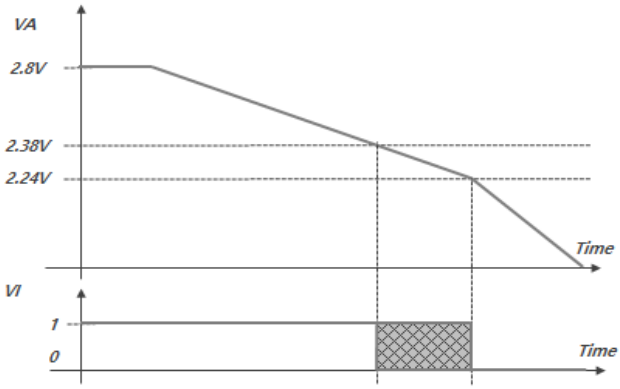


Figure 3. VI Signal Out at Low Voltage Input

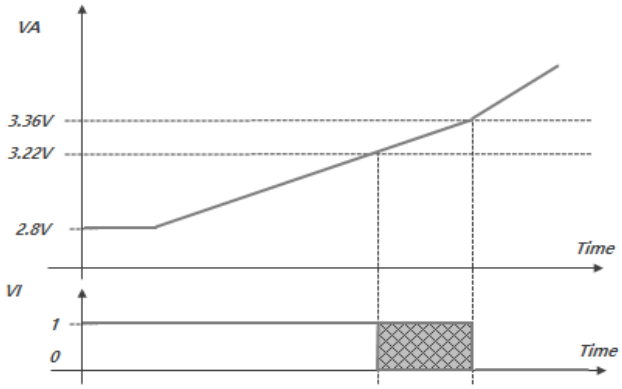


Figure 4. VI Signal Out at High Voltage Input

IDQ6MC1 provides a VI pin for indicating the normality of the input voltage. The VI pin is connected to internal UVD (under voltage detection) and OVD (over voltage detection) circuits. As shown in the above figures, the VI pin remains 'high' for a normal voltage input around 2.8V ± 15% ,otherwise the pin outputs 'low'. When the VI Pin is changed to 'low', the IDQ6MC1 enters into the Dead-Mode and will change back to the Normal-Mode only if the input voltage is on the normal range and the reset command is given from the host device.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

3.2. IDQ6MC1 RNG Data Output Control

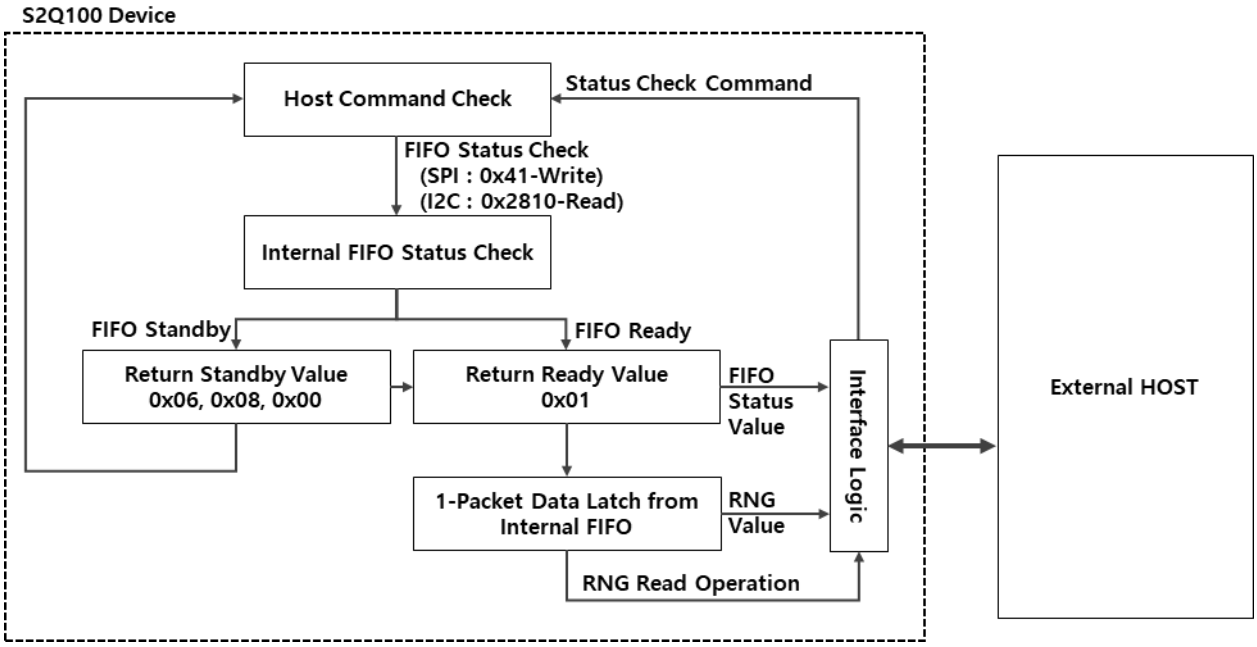


Figure 5. IDQ6MC1 RNG Data Access Flow & RNG Packet Data Architecture

When the FIFO status of IDQ6MC1 is only Ready, the RNG data of IDQ6MC1 can be read as shown in the figure above. FIFO Status Check Command is used to check if the FIFO Status is ready or standby.

IDQ6MC1 supports two types of interfaces, I²C and SPI. In order to use the I²C interface to check the FIFO status, the value at address 0x2810 must be 0x0001. And in order to use the SPI interface, the return value must be 0x0001 when writing 0x41. If the Return value is 0x0001 after the Status Check, the RNG Data value can be read at the end and the 144-bit (including Header) Data is carried out to latch the interface Logic internally.

A user who is using the SPI Interface can read the 1-packet RNG data through the RNG data read implement. A user who is using the I²C interface can read the 1-packet RNG data through reading address 0x2820~0x2830. When 144-bit RNG data is carried out latch to interface logic internally, all the 144-bit RNG data should be read to use the Status Check Command again. Thus, all of 1-packet RNG data should be read in case the FIFO is Ready(0x0001) when the status check is read

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

3.2.1. RNG Data Access with SPI Protocol

- IDQ6MC1 SPI Interface

IDQ6MC1 supports both SPI Interface for high-speed communication and I²C Interface for low-speed communication. SDO data is outputted based on SCK negative edge clock in the protocol of the SPI interface supported by IDQ6MC1. The first data of SDO is MSB bit.

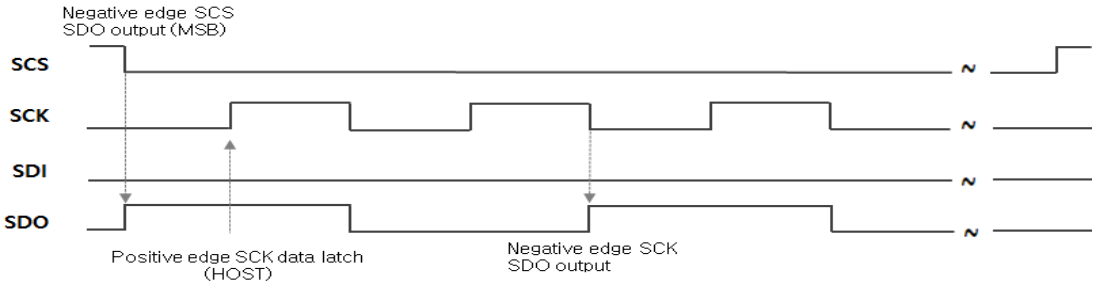
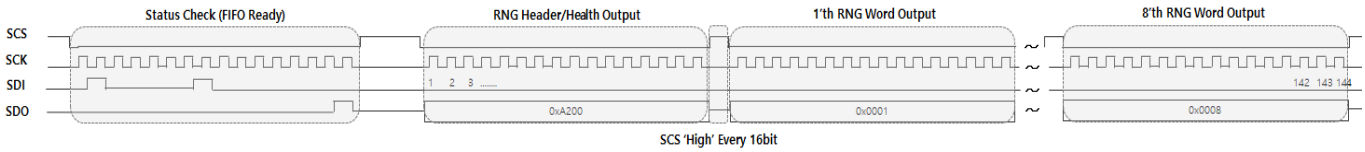


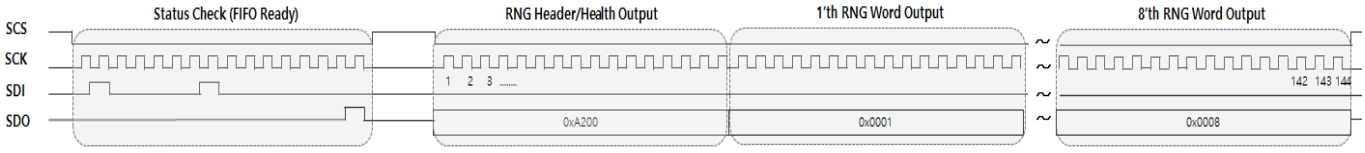
Figure 6. IDQ6MC1 SPI Interface protocol

When the value of MSB bit is '1', SDO data is outputted based on the SCS negative edge as shown in the figure above. A host using IDQ6MC1 should latch the SDO data at the SCK positive edge as above. For details of the timing diagram of the SPI protocol, refer to 'SPI protocol interface timing diagram'.

SPI interface supports Burst mode to maximize Data Throughput, also No Burst and 1~16 Burst mode for hosts' convenience. Burst mode is only used to read the RNG data and it can read 144-bit(1-Packet = 16bit Header/Health & 8-Word RNG data) all at once for each 1-Burst. If the SCS signal remains 'low', it can read 144-bit at once. In case of 16-burst mode, SCS signal can read 2,304-bit (including Header/Health) in the state of 'Low'. Thus, if N Burst is selected, N x 144-bit(1-Packet) can be read and N x 128-bit of the RNG data can be also read.

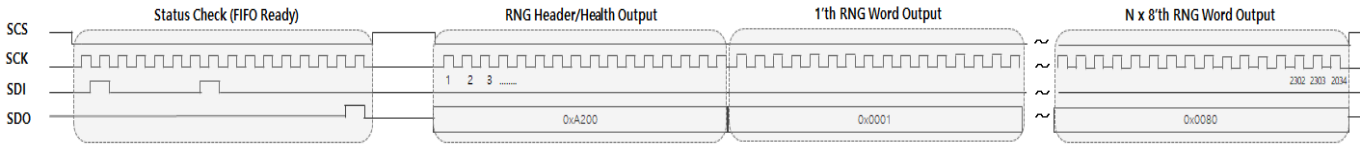


(a) No Burst SPI Mode



(b) 1-Burst SPI Mode

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.



I 16-Burst SPI Mode

Figure 7. IDQ6MC1 SPI Mode Timing Diagram

- FIFO Status Check Operation

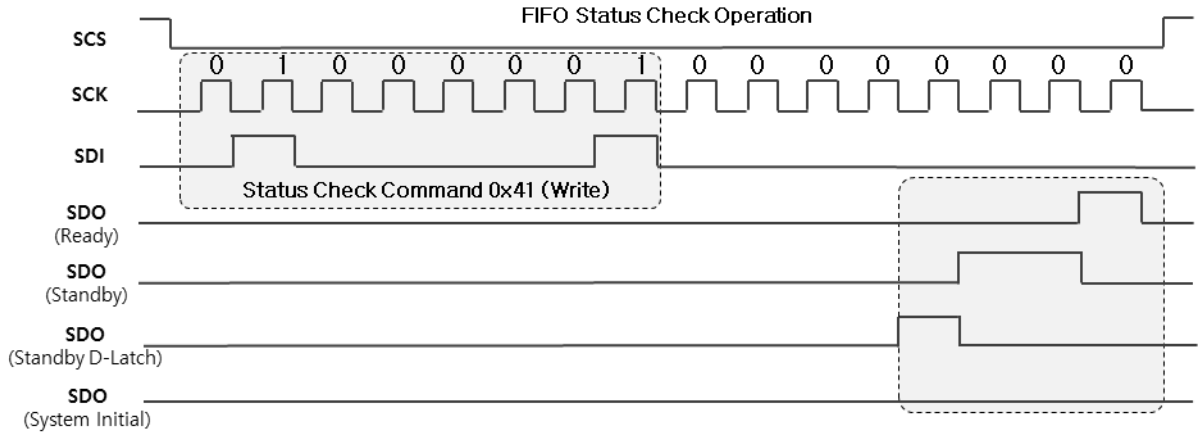


Figure 8. IDQ6MC1 Status Check Timing Diagram in SPI Protocol

In RNG data read mode, IDQ6MC1 allows users to check the RNG FIFO status. When SDI = '0x41' Write, it returns the following four states values. IDQ6MC1 is ready to output the RNG data, only if SDO[3:0] = '0x1'. Otherwise, users should try to check the RNG FIFO status with SDI = '0x41' until IDQ6MC1 returns '0x1'. However, it is necessary for every check to be executed after waiting for at least T_{SCR} (20us).

Status Return Value (LSB-4bit): Ready (0x1)

Ready to output RNG data

!! Notice : If ready(0x1) occurs then the RNG FIFO Read operation should not be performed again.

Status Return Value (LSB-4bit): Standby (0x6)

The system is ready, but still waiting for filling the FIFO with the RNG data

Status Return Value (LSB-4bit): Standby D-Latch (0x8)

The system is ready, and the FIFO data's been uploaded to the SPI interface logic part.

Status Return Value (LSB-4bit): System Ready (0x0)

The System is on and ready to run the QRNG core logic to generate RNG data.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

- 1-Packet RNG Data Read Operation

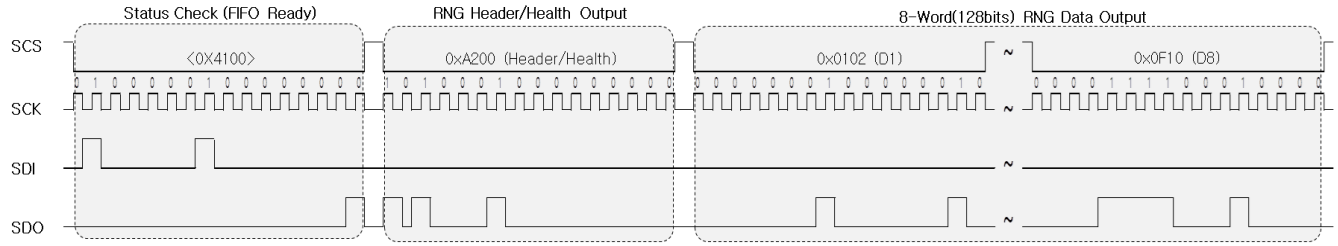


Figure 9. QRNG Data Transfer Timing Diagram (No Burst SPI Mode)

When the FIFO status is Ready (0x1), IDQ6MC1 returns first both header and health information when it receives SDI='0x0000'. The header is a fixed 8-bit string with 0xA2. The health information indicates the normality of the core parts of the chip such as the LED, sensor, noise level, core logic integrity, and the quality of entropy. If it has 0x00, then this means all parts are normally working. After that, IDQ6MC1 outputs 16-bit RNG data whenever SDI='0x0000' is given. After repeating this behavior 8 times, it outputs header and health information again. So, we can regard that IDQ6MC1 outputs in the format of 9 words consisting of one word of the header and health information and 8 words of the RNG data. It is shown figure9.

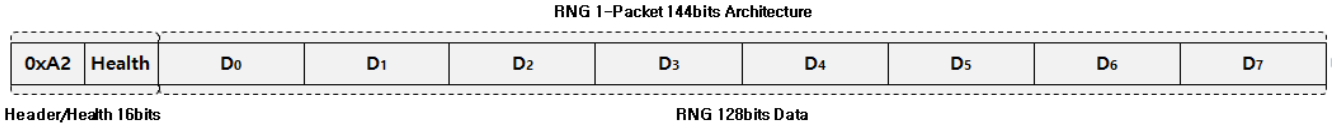


Figure 10. IDQ6MC1 RNG 1-Packet Data Architecture

The FIFO status check could be optional. However, we recommend checking the FIFO status as frequently as possible after reading out the 9-word RNG dataset. This is to prevent from reading RNG data when the FIFO is empty.

Table 2. Health Information

Health Bit	Description
B[7]	Health Check Ready Error
B[6]	RNG Proportion Error
B[5]	RNG Repetition Error
B[4]	Image Max Error
B[3]	Image Min Error
B[2]	Sensor Operation Error
B[1]	LED Operation Error
B[0]	Dark Sum Error

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

3.2.2. RNG Data Access with I²C Interface Protocol

- IDQ6MC1 I²C Interface

IDQ6MC1 has 0x37 (7bit) as a device address for I²C. IDQ6MC1 operates an I²C protocol based on 16-bit address and Data. The following figure represents the I²C data read/write protocol.

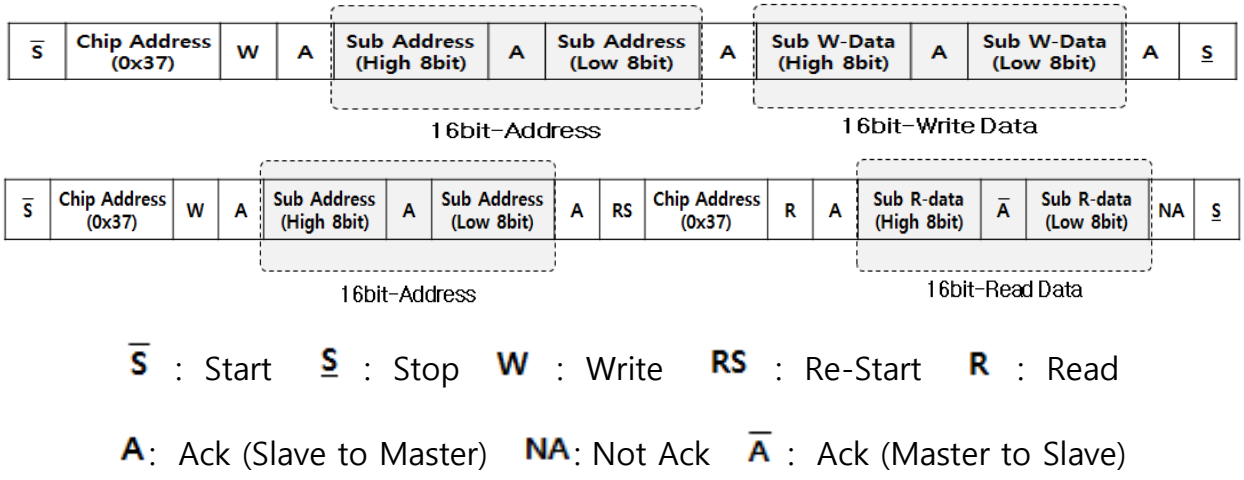


Figure 11. IDQ6MC1 I²C Protocol Write/Read

- FIFO Status Check Operation

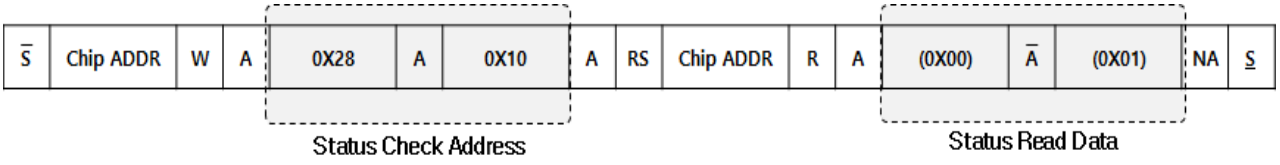


Figure 12. IDQ6MC1 I²C Mode Status Check

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

In RNG data read mode by I²C Protocol, IDQ6MC1 allows users to check the RNG FIFO status. When users read the value at address 0x2810, it returns the following four states values. IDQ6MC1 is ready to output RNG data, only if LSB 4bit = '0x1'. Otherwise, users should try to check the RNG FIFO status with reading the value at address 0x2810 until IDQ6MC1 returns '0x1'. However, it is necessary for every check to be executed after waiting for at least T_{SCR} (20us).

Status Return Value (LSB-4bit): Ready (0x1)

Ready to output RNG data

!! Notice : If ready(0x1) occurs then the RNG FIFO Read operation should not be performed again.

Status Return Value (LSB-4bit): Standby (0x6)

The system is ready, but still waiting for filling the FIFO with the RNG data.

Status Return Value (LSB-4bit): Standby D-Latch (0x8)

The system is ready, and the FIFO data's been uploaded to the SPI interface logic part.

Status Return Value (LSB-4bit): System Ready (0x0)

The system is on and ready to run the QRNG core logic to generate the RNG data.

- 1-Packet RNG Data Read Operation

IDQ6MC1 supports both of a single mode and burst mode for RNG data access. The mode can be chosen by setting the 16-bit address. If the address is 0x2840, IDQ6MC1 outputs a single 16-bit RNG data. Of course, the first word could be both the header and the health information, and the next 8 words will be the RNG data.

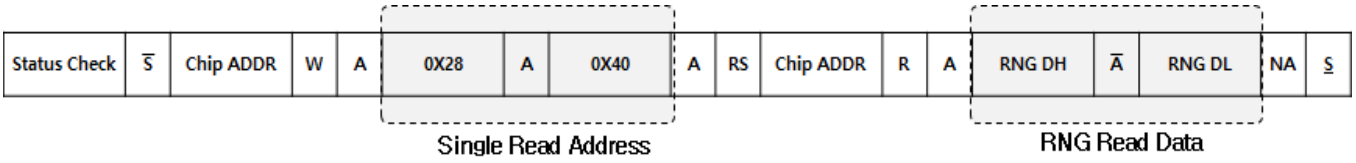


Figure 13. I²C Single Read Mode RNG Data Read

Table 3. I²C Single Read Data Access Address

Address	Description	Default Value
0x2840	B[15:0] : I²C Single Mode RNG Data Output	-

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

However, in the burst mode which operates when the address = '0x2820', IDQ6MC1 will provide the whole 1-Packet (144 bits) dataset at once as follows.

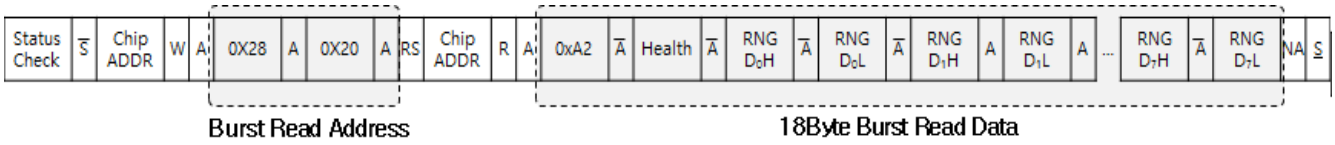


Figure 14. I²C Burst Read Mode RNG Data Read

Table 4. I²C Burst Read Data Access Address

Address	Description	Default Value
0x2820	B[15:0] : I²C Interface Burst Mode Header	-
0x2822	B[15:0] : I²C Interface Burst Mode DATA0	-
0x2824	B[15:0] : I²C Interface Burst Mode DATA1	-
0x2826	B[15:0] : I²C Interface Burst Mode DATA2	-
0x2828	B[15:0] : I²C Interface Burst Mode DATA3	-
0x282A	B[15:0] : I²C Interface Burst Mode DATA4	-
0x282C	B[15:0] : I²C Interface Burst Mode DATA5	-
0x282E	B[15:0] : I²C Interface Burst Mode DATA6	-
0x2830	B[15:0] : I²C Interface Burst Mode DATA7	-

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

3.3. Sample Noise Data Output Mode in SPI Protocol

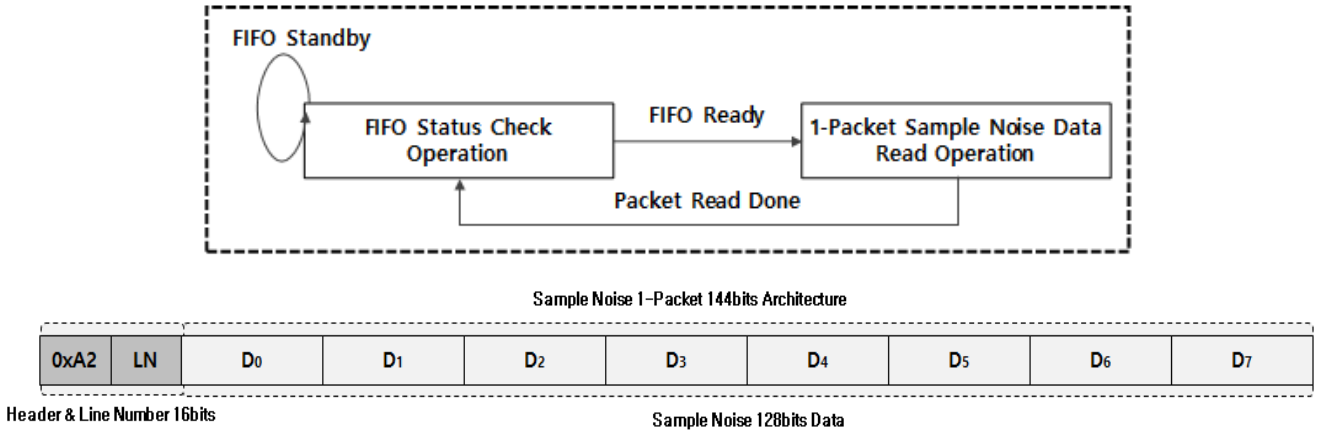


Figure 15. IDQ6MC1 Sample Noise Data Access Flow & Sample Noise Packet Data Architecture

IDQ6MC1 also allows itself to access the entropy data instead of the RNG data. The entropy data is sometimes called a noise sample data, because it is sampled from the analog noise. The sample data is 4 times bigger than the RNG data. Actually, IDQ6MC1 produces the sample data at the speed of 6Mbps. Therefore, in order to read all the sample data from IDQ6MC1 without any loss, it requires a high-speed interface sufficiently faster than 6Mbps. So, IDQ6MC1 supports the sample data output in the SPI interface mode.

All setting and processing methods for accessing the sample data is same with that for accessing the RNG data. However, the sample data has totally different data format from the RNG data. It has no health-related information, but it instead has the line number (LN) as follow. The LN indicates the row number of the active pixel array the sample data taken from. Since each pixel produces 2-bit sample, each row requires the capacity of 256 bits (= 128 x 2 bits). Therefore, in the 9-word format, the LN will be repeated two times.

0xA201	D0	D1	D2	D3	D4	D5	D6	D7	0xA201	D8	D9	D10	D11	D12	D13	D14	D15
0xA202	D16	D17	D18	D19	D20	D21	D22	D23	0xA202	D24	D25	D26	D27	D28	D29	D30	D31
0xA203	D32	D..	D..	D..	D..	D..	D..	D..	0xA203	D..	D..	D..	D..	D..	D..	D..	D47
⋮															⋮		
0xA264	D1584	D..	D..	D..	D..	D..	D..	D..	0xA264	D..	D..	D..	D..	D..	D..	D..	D1599

Figure 16. QRNG Sample Mode Output Data Format

Sample noise data in IDQ6MC1 is generated independently from the FIFO Index. Therefore, in order to access the continuous sample noise data, it is necessary to access faster than the IDQ6MC1 sample noise generation speed.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

4. Physical Specifications

4.1. Absolute Maximum Ratings

	MIN	MAX	UNIT
Voltage Applied at VA	-0.3	4.5	V
Voltage Applied to any pin	-0.3	4	V
Diode Current at any device pin		±2	mA
Operating Temperature (TBD)	-40	125	℃
Stable Quality Temperature (TBD)	-30	85	℃

4.2. ESD Ratings

		VALUE	UNIT
$V_{(ESD)}$ Electrostatic discharge	Human-body model (HBM)	±2000	V
	Charged-device model (CDM)	±700	

4.3. Operation Voltage

	MIN	TYP	MAX	UNIT
1.8V I/O Voltage (VDDIO)	1.65	1.8	1.95	V
2.8V Supply Voltage (VA)	2.38	2.8	3.22	

4.4. I/O DC Characteristics

	MIN	TYP	MAX	UNIT
Input Low Voltage (VIL)	-0.3	-	0.3xVDDIO	V
Input High Voltage (VIH)	0.7xVDDIO	-	4	V
Output Low Voltage (VOL)		-	0.2	V
Output High Voltage (VOH)	VDDIO-0.2	-	-	V
Low Level Output Current at VOL=0.2 (IOL)	-	-	-200	uA
High Level Output Current at VOH=VDD-0.2 (IOH)	200uA	-	-	uA

Note: Pull-up mode voltage level of VOH is 0.8 x VDDIO

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

4.5. Recommended Interface Frequency Ranges

	MIN	TYP	MAX	UNIT
SPI Protocol	6		24	MHz
I²C Protocol	10		100	KHz

4.6. Power Consumption in Operation Modes

	MIN	TYP	MAX	UNIT
Normal Mode (generating random bits)	56.9		59.94	mW
Sample Noise Output Mode	56.2		58.24	mW

4.7. Timing and Switching Characteristics

4.7.1. Power Up Timing with External VDD Source

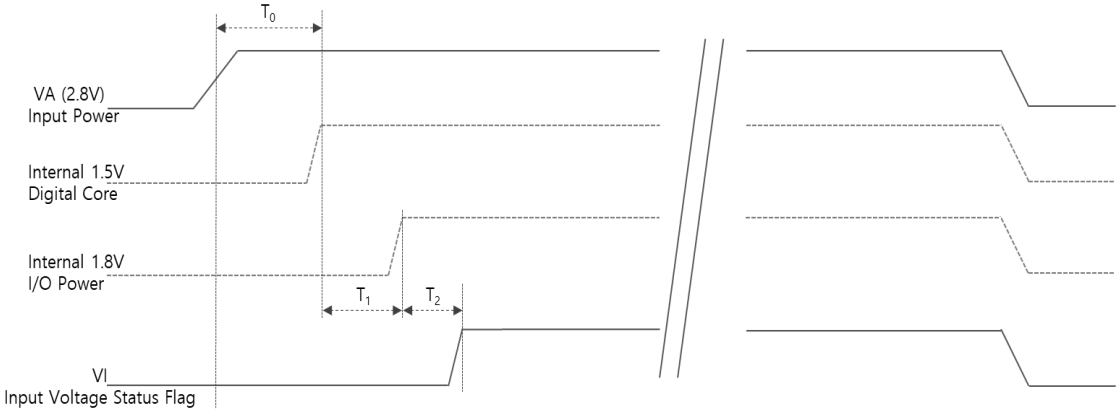


Figure 17. IDQ6MC1 Power Up/Down Timing Diagram

Table 5. IDQ6MC1 Power Up/Down Timing Parameter

Parameter	Min	Typ	Max
Core Voltage Wakeup Timing (T_0)	20.0us	-	21.0us
I/O Voltage Wakeup Timing (T_1)	1.0us	-	2.0us
VI Pin Stabilization Timing (T_2)	3us	-	4.0us

Note: This value is based on VA(1.4V) 50% point

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

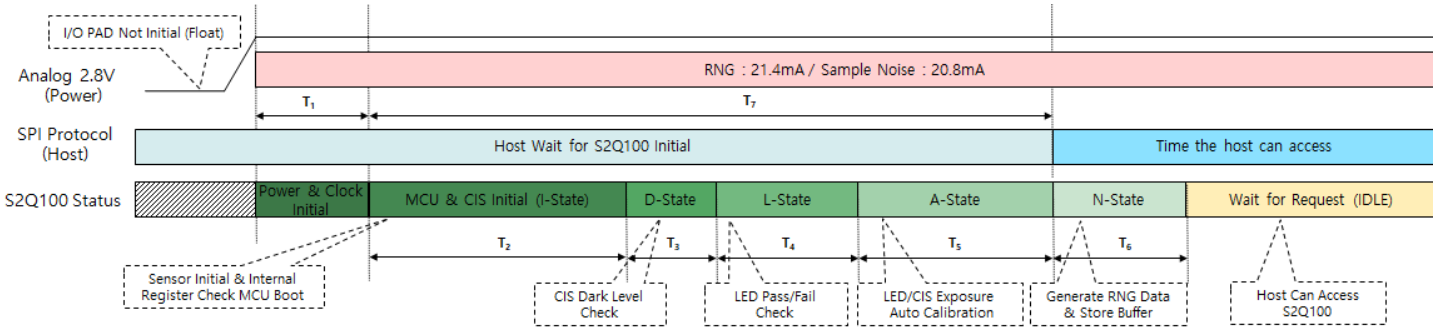


Figure 18. IDQ6MC1 Internal Initial Setup Time & Power Consumption

Table 6. IDQ6MC1 Internal Initial Setup Timing Parameter

Parameter	Min	Typ	Max
Power Up Initial Setup Time (T_1)	24.0us	27.0us	30.0us
Internal CIS/MCU Setup Time (T_2)**	90.0ms	100.0ms	-
CIS Dark Level Check Setup Timing (T_3)	3.32ms	4.14ms	4.77ms
LED Pass/Fail Check Setup Timing (T_4)	19.84ms	24.8ms	28.52ms
LED/CIS Auto Calibration Setup Timing (T_5)	32.2ms	41.4ms	47.7ms
RNG Data Generation Setup Timing (T_6)	26.48ms	33.1ms	38.06ms
IDQ6MC1 Standby Time Timing (T_7)	145.36ms	170.3ms	-

** T_2 : CIS/MCU Setup Time is may vary depending on mode and setting value.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

4.7.2. SPI Protocol Interface Timing Diagram

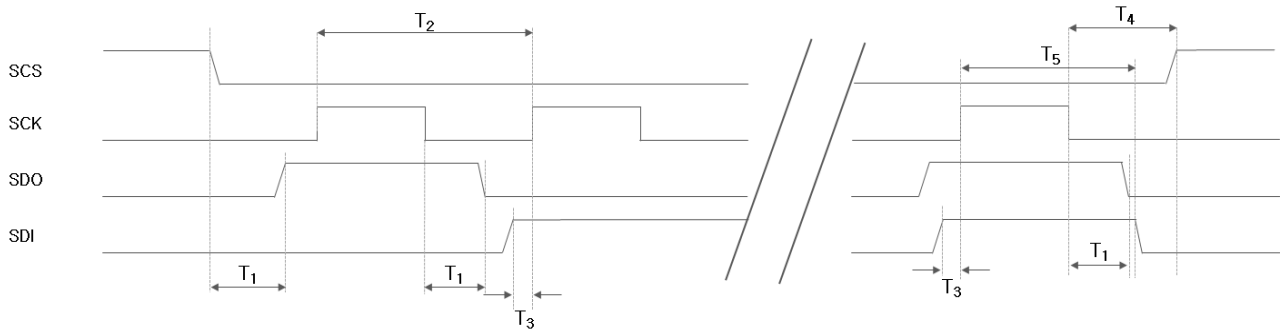


Figure 19. SPI Protocol Interface Timing Diagram

The IDQ6MC1 SPI Slave Protocol outputs SDO based on the SCK Negative Edge. It is designed to latch the SDI signal based on the SCK positive edge.

Table 7. IDQ6MC1 SPI Protocol Interface Timing Parameter

Parameter	Min	Typ	Max
SDO Output Response Time (T_1)	8.2 ns	10.0 ns	14.0 ns
SCK Duration Time (T_2)	37.03 ns	-	166.6 ns
SDI Input Setup Time (T_3)	4 ns	-	-
SCK to SCS Rising Time (T_4)	18.51 ns	-	333.2 ns
SCK to SCS Rising Time (T_4*)	1.3us	-	
SDI Input Hold Time (T_5)	0 ns	-	-

T_4* : if host use a protocol with a long 'SCS' low section.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

4.7.3. IDQ6MC1 FIFO Status Check & QRNG Data Read Timing in SPI Protocol

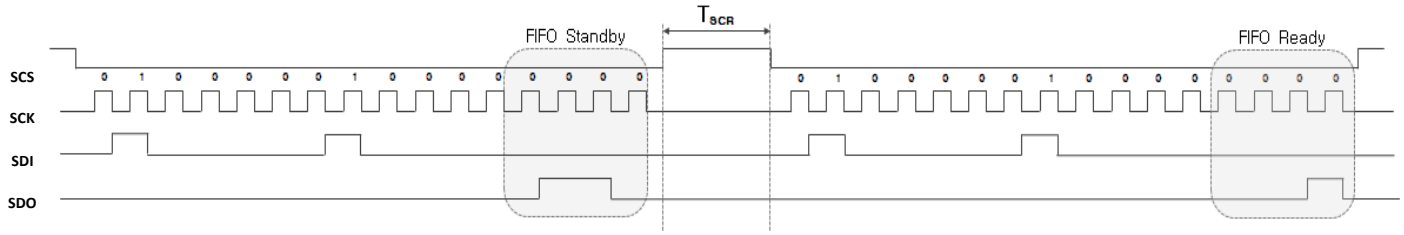


Figure 20. IDQ6MC1 FIFO Status Check Timing Diagram in SPI Protocol (FIFO Ready after FIFO Standby)

Table 8. IDQ6MC1 Repetition Status Check Timing Parameter in SPI Protocol

Parameter	Min	Typ	Max
T_{SCR} (Status Check Retiming)	20.0us	-	-

To access the IDQ6MC1 RNG data, check first whether the RNG FIFO is ready. T_{SCR} is the time required to make the SPI Slave Interface Logic usable, that is, to transit the FIFO state inside the chip from the Standby state to the Ready state. If the FIFO Status is in Standby, then it is recommended to check the FIFO status again after T_{SCR} time.

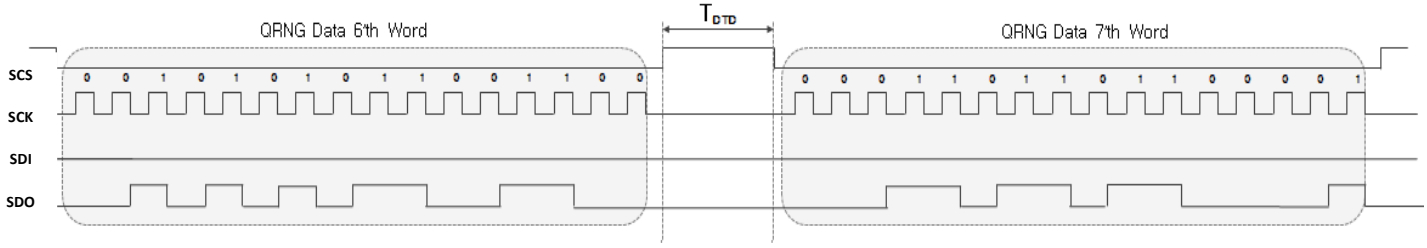


Figure 21. QRNG Data Read Timing Diagram

Table 9. QRNG Data Read Latency Timing Parameter in SPI Protocol

Parameter	Min	Typ	Max
T_{DTD} (Data Read to Data Read)	250ns	-	-

Under the FIFO Ready state and data output mode, the IDQ6MC1 outputs 16-bit data, whenever the transition of SCS occurs, in the order as Header (8bit) + Health (8bit), RNG 1st (16bit), … , RNG 8th (16bit), Header (8bit) +

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

Health (8bit), RNG 1st (16bit), and so on. At this time, at least T_{DTD} waiting time is required for memory access and asynchronous clock processing in order to switch the data in the FIFO. So, the SPI master (host) generates a SCS signal in 'high' at least T_{DTD} duration. In addition, it is recommended to read 9-word (16-bit data) consecutively to distinguish between the header information and the RNG data. If using the SPI Burst Mode to read the RNG data then T_{DTD} time is zero.

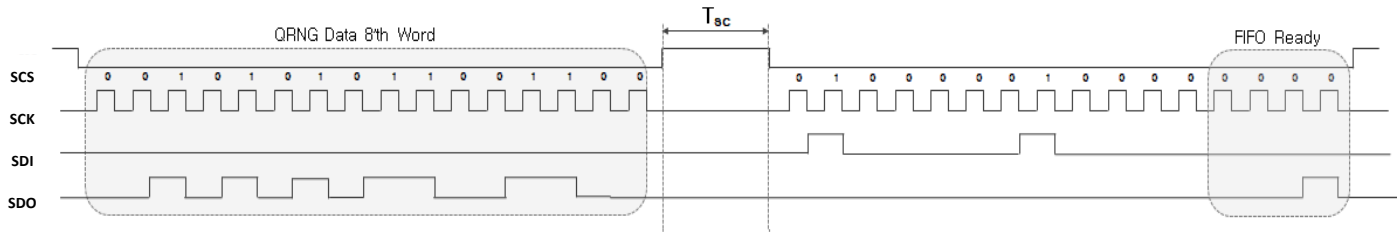


Figure 22. IDQ6MC1 Status Check Timing Diagram in SPI Protocol (FIFO Ready after QRNG Data Read Done)

Table 10. IDQ6MC1 Status Check Timing Parameter in SPI Protocol

Parameter	Min	Typ	Max
T_{SC} (Status Check after data read done)	250ns	-	-

Every time after reading 9 consecutive words consisting of header and 8 RNG words, it is necessary to check the FIFO status. The reason for this is to figure out whether the FIFO is empty or not. T_{SC} is the minimum time required for the FIFO Status Check after the RNG data Access.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

4.7.4. I²C Timing Diagram

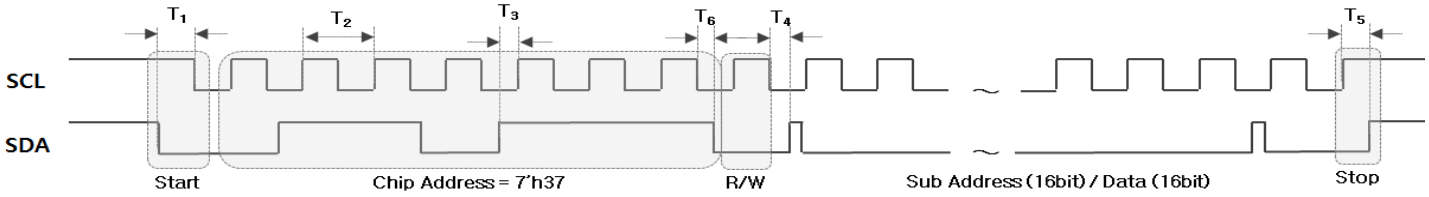


Figure 23. IDQ6MC1 I²C Protocol Timing Diagram

Table 11. IDQ6MC1 I²C Timing Parameter in I²C Protocol

Parameter	Min	Max
T_1 (Serial Data to Serial Clock Setup Time)	500ns	-
T_2 (Serial Clock Duration)	10us	-
T_3 (Serial Data Setup Time)	500ns	-
T_4 (Serial Data Acknowledge Time)	4us	-
T_5 (Serial Clock to Serial Data Setup Time)	500ns	-
T_6(Negative Serial Clock Data Hold Time)	334ns	-

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

5. Applications Circuits

5.1. IDQ6MC1 SPI Interface Reference Circuit

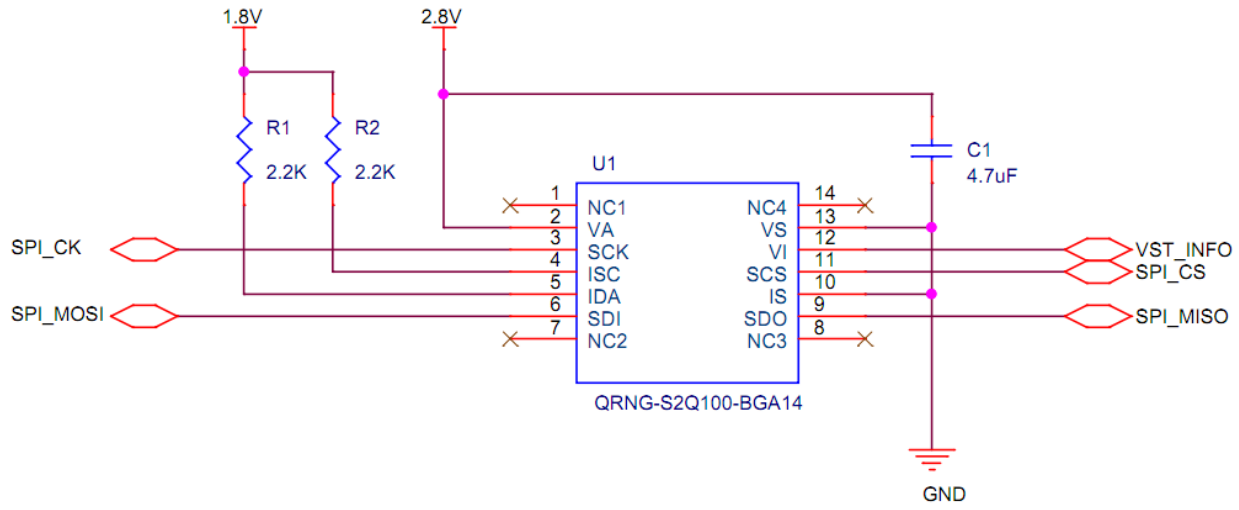


Figure 24. IDQ6MC1 SPI Protocol Reference Circuit

Table 12. IDQ6MC1 SPI Protocol Pin Description

Pin Number	Pin Name	Pin Configuration	Description
2	VA	2.8V	2.8V (2.38V ~ 3.22V)
3	SCK	INPUT	SPI Slave Clock Input
4	ISC	1.8V	1.8V (2.2K option)
5	IDA	1.8V	1.8V (2.2K option)
6	SDI	INPUT	SPI Slave Data Input (MOSI)
9	SDO	OUTPUT	SPI Slave Data Output (MISO)
10	IS	GND	SPI Protocol Selection
11	SCS	INPUT	SPI Slave Chip Selection
12	VI	OUTPUT	QRNG Voltage Status Information Flag
13	GND	GND	Chip Ground
1,7,8,14	NC	NC	NC

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

5.2. I²C Interface Reference Circuit

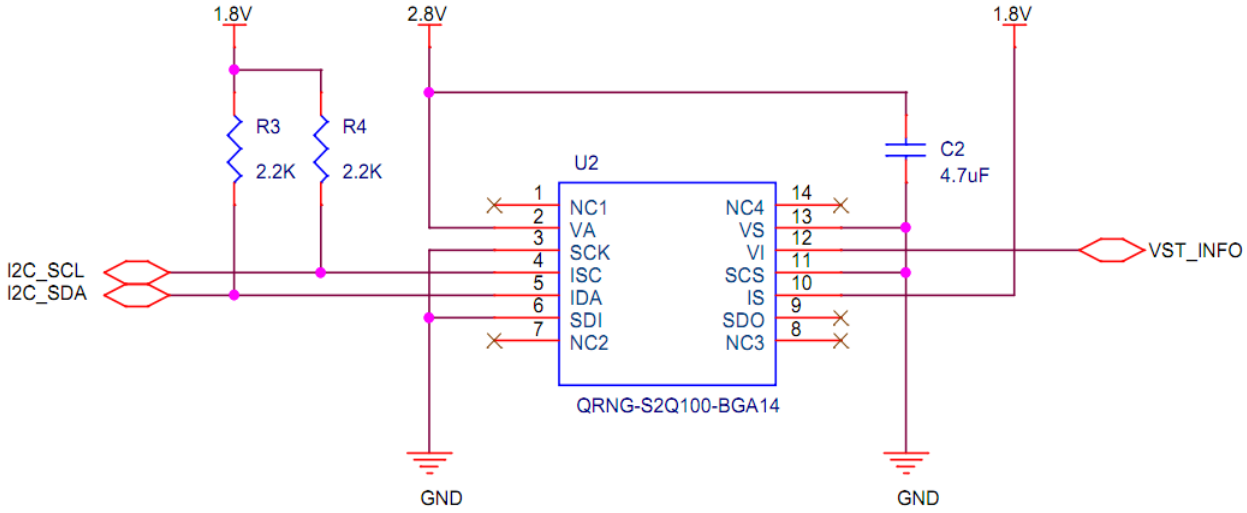


Figure 25. IDQ6MC1 I²C Protocol Reference Circuit

Table 13. IDQ6MC1 I²C Protocol Pin Description

Pin Number	Pin Name	Pin Configuration	Description
2	VA	2.8V	2.8V (2.38V ~ 3.22V)
3	SCK	GND	GND
4	ISC	1.8V	I²C Serial Clock Input
5	IDA	1.8V	I²C Serial Data In/Out
6	SDI	GND	GND
9	SDO	NC	NC
10	IS	1.8V	I²C Mode Selection
11	SCS	INPUT	GND
12	VI	OUTPUT	QRNG Voltage Status Information Flag
13	GND	GND	Chip Ground
1,7,8,14	NC	NC	NC

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

5.3. Multi-Chip Interface Guide

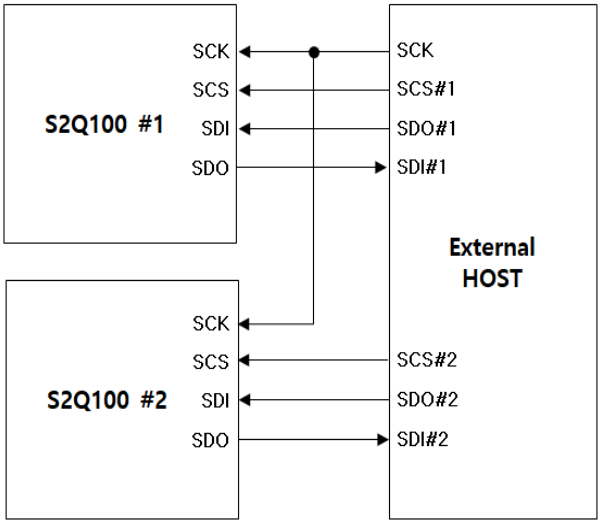


Figure 26. IDQ6MC1 Multi-Chip Interface [Parallel Mode]

The figure above shows a circuit system that uses two IDQ6MC1 chips to increase throughput. As IDQ6MC1 has an internal ROSC, a LED and others inside, each chip does not have same operating frequency and optical effect. Thus, in case of using multi IDQ6MC1 chips, it is recommended to control independently except SCK as shown above.

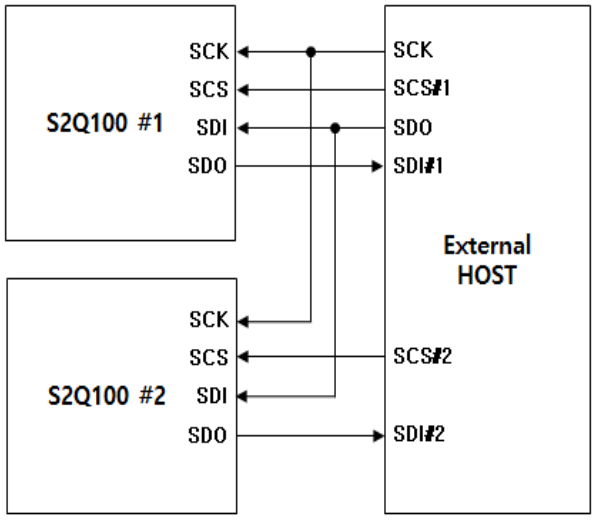


Figure 27. IDQ6MC1 Multi-Chip Interface [Parallel Mode Common SDI]

The figure above shows a circuit system that uses two IDQ6MC1 chips simultaneously to share SDI pin. There is a bigger loss throughput with this circuit compared to Figure 26, because two chips are controlled

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.

independently as previously stated. The FIFO ready time can be different. And RNG data cannot be read until two chips are ready to read the RNG data at the same time because the RNG data can be read after the state of FIFO ready. If the chip in the state of ready must read the RNG data, the input signal of SCS should be 'High' when commanding the FIFO Status Check of the chip in the state of not ready.

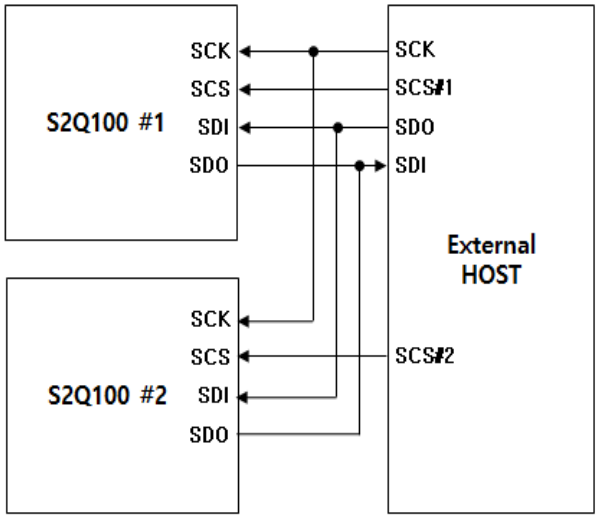


Figure 28. IDQ6MC1 Multi-Chip Interface [Serial Mode]

The figure above shows a circuit system when using two IDQ6MC1 chips simultaneously to share the SDI and the SDO pins. Compared to the two previous circuits, this circuit has the biggest loss. There is the biggest loss throughput with this circuit compared to Figure 26 and 27. In case of using this circuit system, another chip should retain SCS with 'High' when reading the RNG data. IDQ6MC1 can share the output line if the SDO is in the state of Hi-Z when the input signal of the SCS is 'High'.

CONFIDENTIAL. This document and any data included are the property of ID Quantique. They cannot be reproduced, disclosed or utilized without the company's prior written approval.