DS1964S

DeepCover Secure Authenticator iButton with SHA-256

General Description

DeepCover® embedded security solutions cloak sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible.

The DeepCover Secure Authenticator iButton® (DS1964S) combines crypto-strong bidirectional secure challenge-and-response authentication functionality with an implementation based on the FIPS 180-3-specified Secure Hash Algorithm (SHA-256). A 512-bit user-programmable EEPROM array provides nonvolatile storage of application data. Additional protected memory holds a read-protected secret for SHA-256 operations and settings for memory protection control. Each device has its own guaranteed unique 64-bit ROM identification number (ROM ID) that is factory programmed into the chip. This unique ROM ID is used as a fundamental input parameter for cryptographic operations and also serves as an electronic serial number within the application. A bidirectional security model enables two-way authentication between a host system and slave-embedded DS1964S. Slave-to-host authentication is used by a host system to securely validate that an attached or embedded DS1964S is authentic. The DS1964S communicates over the single-contact 1-Wire® bus at overdrive speed. The communication follows the 1-Wire protocol with the ROM ID acting as node address in the case of a multidevice 1-Wire network.

Applications

Authentication of Consumables

Secure Feature Control

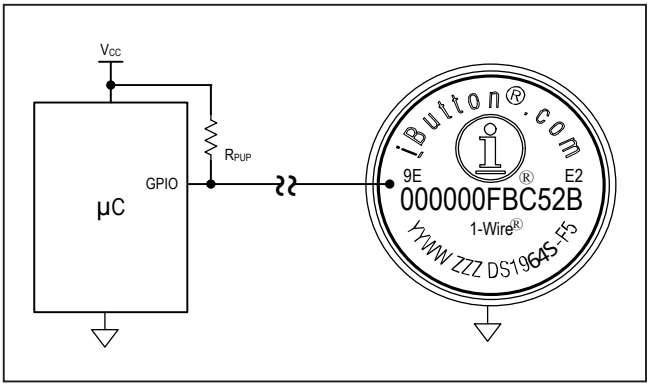
Examples of Accessories

PART	ACCESSORY
DS9093RA	Mounting Lock Ring
DS9093A	Snap-in FOB
DS9092	iButton Probe
DS1402D-DR8+	Blue Dot Receptor Cable

Features

- Symmetric-Key-Based Bidirectional Secure Authentication Model Based on SHA-256
- Strong Authentication with a High-Bit-Count User-Programmable Secret and Input Challenge
- 512 Bits of User EEPROM Partitioned Into Two Pages of 256 Bits
- User-Programmable and Irreversible EEPROM Protection Modes Including Write and Read Protect and OTP/EPROM Emulation
- Unique Factory-Programmed, 64-Bit Identification Number
- Single-Contact 1-Wire Interface
- Operating Range: -40°C to +85°C
- ±8kV HBM ESD Protection (typ)
- Durable Stainless-Steel Enclosure Withstands Harsh Environments and Conditions

Typical Application Circuit



***Ordering Information* appears at end of data sheet.**

DeepCover, iButton, and 1-Wire are registered trademarks of Maxim Integrated Products, Inc..

19-100347; Rev 0; 6/18

maxim integrated™

Absolute Maximum Ratings

IO Voltage Range to GND.....-0.5V to +4.0V
IO Sink Current.....20mA
Operating Temperature Range..... -40°C to +85°C
Junction Temperature .....+150°C
Storage Temperature Range..... -55°C to +125°C

Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of the specifications is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Electrical Characteristics

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
IO PIN: GENERAL DATA						
1-Wire Pullup Voltage	V_{PUP}	(Note 2)	2.97		3.63	V
1-Wire Pullup Resistance	R_{PUP}	V_{PUP} = 3.3V ±10% (Note 3)	300		1500	Ω
Input Capacitance	C_{IO}	(Notes 4, 5)		1500		pF
Input Load Current	I_L	IO pin at V_{PUP}		5	19.5	µA
High-to-Low Switching Threshold	V_{TL}	(Notes 6, 7)		0.65 x V_{PUP}		V
Input Low Voltage	V_{IL}	(Notes 2, 8)			0.3	V
Low-to-High Switching Threshold	V_{TH}	(Notes 6, 9)		0.75 x V_{PUP}		V
Switching Hysteresis	V_{HY}	(Notes 6, 10)		0.3		V
Output Low Voltage	V_{OL}	I_{OL} = 4mA (Note 11)			0.4	V
Recovery Time	t_{REC}	R_{PUP} = 1500Ω (Notes 2, 12)	5			µs
Time Slot Duration	t_{SLOT}	(Notes 2, 13)	13			µs
IO PIN: 1-Wire RESET, PRESENCE-DETECT CYCLE						
Reset Low Time	t_{RSTL}	(Note 2)	48		80	µs
Reset High Time	t_{RSTH}	(Note 14)	48			µs
Presence-Detect Sample Time	t_{MSP}	(Notes 2, 15)	8		10	µs
IO PIN: 1-Wire WRITE						
Write-Zero Low Time	t_{W0L}	(Notes 2, 16)	8		16	µs
Write-One Low Time	t_{W1L}	(Notes 2, 16)	1		2	µs
IO PIN: 1-Wire READ						
Read Low Time	t_{RL}	(Notes 2, 17)	1		2 - δ	µs
Read Sample Time	t_{MSR}	(Notes 2, 17)	t_{RL} + δ		2	µs

Electrical Characteristics (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
EEPROM						
Programming Current	I_{PROG}	V_{PUP} = 3.63V (Notes 5, 18)			1	mA
Programming Time for a 32-Bit Segment or Page Protection	t_{PRD}	(Note 19)			10	ms
Programming Time for the Secret	t_{PRS}	(Note 20)			100	ms
Write/Erase Cycling Endurance	N_{CY}	T_A = +85°C (Notes 21, 22)	100k			—
Data Retention	t_{DR}	T_A = +85°C (Notes 23, 24, 25)	10			Years
SHA-256 ENGINE						
Computation Current	I_{CSHA}	V_{PUP} = 3.63V (Notes 5, 18)			1	mA
Computation Time	t_{CSHA}	(Note 26)			3	ms

Note 1: Limits are 100% production tested at T_A = +25°C and/or T_A = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are not guaranteed.
Note 2: System requirement.
Note 3: Maximum allowable pullup resistance is a function of the number of 1-Wire devices in the system and 1-Wire recovery times. The specified value here applies to systems with only one device and with the minimum 1-Wire recovery times.
Note 4: Typical value represents the internal parasite capacitance when V_{PUP} is first applied. Once the parasite capacitance is charged, it does not affect normal communication.
Note 5: Guaranteed by design and/or characterization only. Not production tested.
Note 6: V_{TL}, V_{TH}, and V_{HY} are a function of the internal supply voltage, which is a function of V_{PUP}, R_{PUP}, 1-Wire timing, and capacitive loading on IO. Lower V_{PUP}, higher R_{PUP}, shorter t_{REC}, and heavier capacitive loading all lead to lower values of V_{TL}, V_{TH}, and V_{HY}.
Note 7: Voltage below which, during a falling edge on IO, a logic 0 is detected.
Note 8: The voltage on IO must be less than or equal to $V_{IL(MAX)}$ at all times the master is driving IO to a logic 0 level.
Note 9: Voltage above which, during a rising edge on IO, a logic 1 is detected.
Note 10: After V_{TH} is crossed during a rising edge on IO, the voltage on IO must drop by at least V_{HY} to be detected as logic 0.
Note 11: The I-V characteristic is linear for voltages less than 1V.
Note 12: Applies to a single device attached to a 1-Wire line.
Note 13: Defines maximum possible bit rate. Equal to $1/(t_{W0L(MIN)} + t_{REC(MIN)})$.
Note 14: An additional reset or communication sequence cannot begin until the reset high time has expired.
Note 15: Interval after t_{RSTL} during which a bus master can read a logic 0 on IO if there is a DS1964S present. The power-up presence detect pulse could be outside this interval but will be complete within 2ms after power-up.
Note 16: ε in Figure 6 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to V_{TH}. The actual maximum duration for the master to pull the line low is $t_{W1L(MAX)} + t_F - \varepsilon$ and $t_{W0L(MAX)} + t_F - \varepsilon$, respectively.
Note 17: δ in Figure 6 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to the input-high threshold of the bus master. The actual maximum duration for the master to pull the line low is $t_{RL(MAX)} + t_F$.
Note 18: Current drawn from IO during the EEPROM programming interval or SHA-256 computation. The pullup circuit on IO during the programming interval or SHA-256 computation should be such that the voltage at IO is greater than or equal to 2.0V.
Note 19: The t_{PRD} interval begins immediately after the trailing rising edge on IO for the last time slot of the release byte for a valid Write Memory and Write Block Protection sequence. The interval ends once the device's self-timed EEPROM programming cycle is complete and the current drawn by the device has returned from I_{PROG} to I_L.
Note 20: The t_{PRS} interval begins immediately after the trailing rising edge on IO for the last time slot of the release byte for a valid Load and Lock Secret sequence and immediately after the second t_{CSHA} for a valid Compute and Lock Secret sequence. The interval ends once the device's self-timed EEPROM programming cycle is complete and the current drawn by the device has returned from I_{PROG} to I_L. Refer to the Security Users Guide for more details on the Load and Lock Secret and Compute and Lock Secret commands.
Note 21: Write-cycle endurance is tested in compliance with JESD47G.
Note 22: Not 100% production tested; guaranteed by reliability monitor sampling.

Electrical Characteristics (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

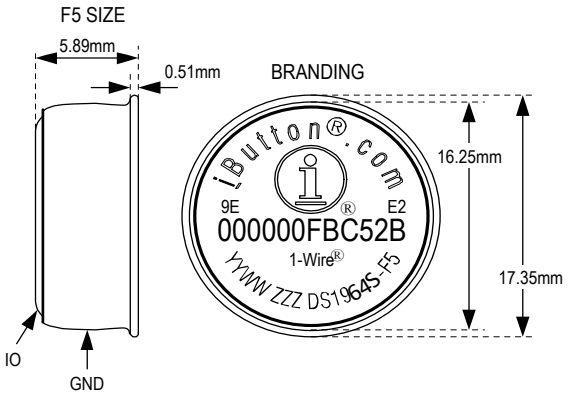
Note 23: Data retention is tested in compliance with JESD47G.

Note 24: Guaranteed by 100% production test at elevated temperature for a shorter time; equivalence of this production test to the data sheet limit at operating temperature range is established by reliability testing.

Note 25: EEPROM writes can become nonfunctional after the data-retention time is exceeded. Long-term storage at elevated temperatures is not recommended.

Note 26: The t_{CSHA} interval begins immediately after the trailing rising edge on IO for the last time slot of the Release byte for a valid Compute and Lock Secret sequence, immediately after the trailing rising edge on IO for the last time slot of the first CRC-16 of a Compute and Read Page MAC sequence. Interval ends once the device's self-timed SHA-256 computation cycle is complete and the current drawn by the device has returned from I_{CSHA} to I_L. The commands Compute and Read Page MAC and Compute and Lock Secret require 2 x t_{CSHA}.

Pin Configuration



Pin Description

NAME	FUNCTION
IO	Input/Output
GND	Ground

Detailed Description

The DS1964S combines a SHA-256 engine with a 256-bit secret, 512 bits of user EEPROM organized as two 256-bit pages, 8 bytes of status memory, and a 64-bit ROM ID in a single chip. A 256-bit scratchpad assists when installing a new secret or stores the challenge when computing a page MAC. Data is transferred serially through the 1-Wire protocol, which requires only a single data lead and a ground return.

There are multiple programmable options for the 512 bit user array including unrestricted read/write and four protection modes: 1) read protection, 2) write protection and 3) EPROM emulation mode. Read protection prevents user read-access to the memory, which effectively converts the protected memory into a secret. The data remains accessible only for the SHA-256 engine. Write protection prevents changes to the memory data. EPROM emulation mode logically ANDs memory data with incoming new data, which allows changing bits from 1 to 0, but not vice versa. By changing one bit at a time this mode could be used to create a nonvolatile nonresettable counter. EPROM emulation mode requires that the memory is not write protected.

In addition to its important use as a unique data value in cryptographic SHA-256 computations, the device's 64-bit ROM ID can be used to electronically identify the equipment in which the DS1964S is used. The ROM ID guarantees unique identification and is also used to address the device in a multidrop 1-Wire network environment, where multiple devices reside on a common 1-Wire bus and operate independently of each other. Applications of the DS1964S are authentication and control of consumables.

Overview

The block diagram in Figure 1 shows the relationships between the major control and memory sections of the DS1964S. The DS1964S has six main data components: two 256-bit pages of user EEPROM, one 256-bit EEPROM secret, eight bytes of status memory, a 512-bit SHA-256 engine, a 64-bit ROM ID and a 256-bit scratchpad. Figure 2 shows the hierarchic structure of the 1-Wire protocol. The bus master must first provide one of the five ROM function commands: Read ROM, Match ROM, Search ROM, Skip ROM, and Resume Communication. The protocol required for these ROM function commands is described in Figure 4. After a ROM function command is successfully executed, the memory and SHA-256 functions become accessible and the master can provide any one of the available memory and SHA function commands. The function protocols are described in the Security Users Guide. **All data is read and written least significant bit first.**

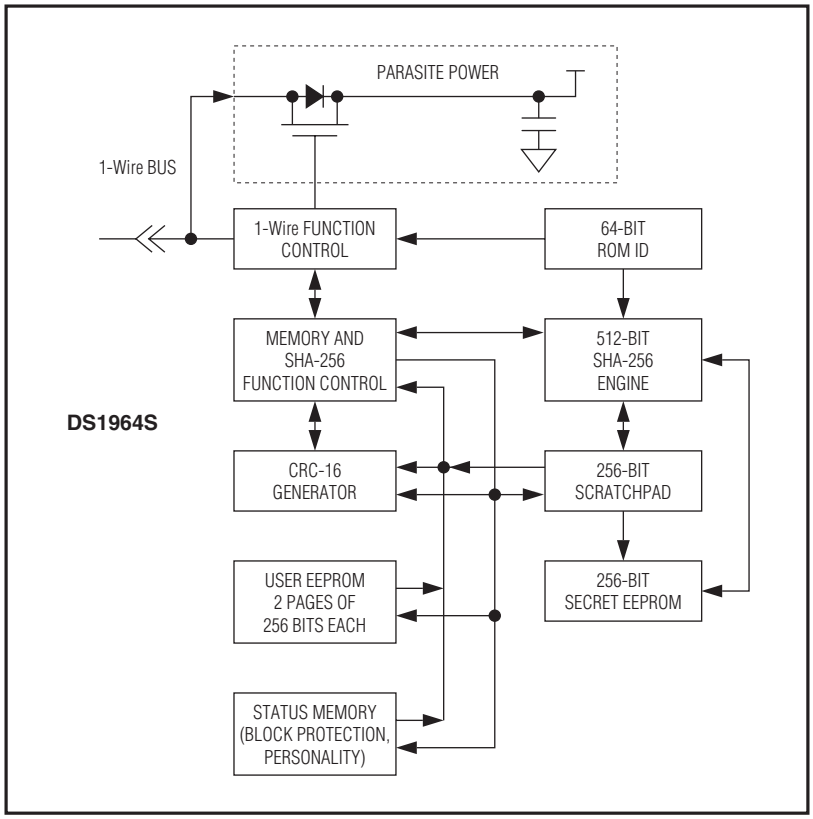


Figure 1. Block Diagram

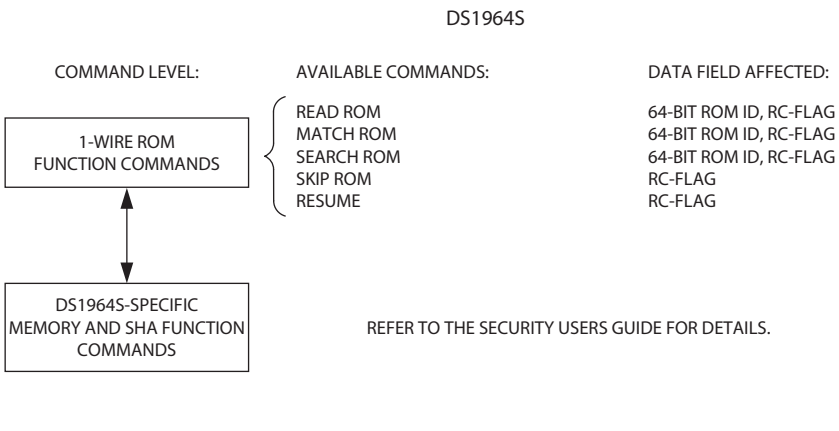


Figure 2. Hierarchical Structure for 1-Wire Protocol

1-Wire Bus System

The 1-Wire bus is a system that has a single bus master and one or more slaves. In all instances the DS1964S is a slave device. The discussion of this bus system is broken down into three topics: hardware configuration, transaction sequence, and 1-Wire signaling (signal types and timing). The 1-Wire protocol defines bus transactions in terms of the bus state during specific time slots, which are initiated on the falling edge of sync pulses from the bus master.

Hardware Configuration

The 1-Wire bus has only a single line by definition; it is important that each device on the bus be able to drive it at the appropriate time. To facilitate this, each device attached to the 1-Wire bus must have open-drain or three-state outputs. The 1-Wire port of the DS1964S is open drain with an internal circuit equivalent to that shown in Figure 3.

A multidrop bus consists of a 1-Wire bus with multiple slaves attached. The DS1964S supports overdrive speed of 76.9kbps (max) only and cannot be used together with standard speed or dual-speed 1-Wire slaves on the bus. The value of the pullup resistor primarily depends on the 1-Wire pullup voltage, network size and load conditions. The DS1964S requires a pullup resistor of maximum 1.5kΩ.

The idle state for the 1-Wire bus is high. If for any reason a transaction must be suspended, the bus must be left in the idle state if the transaction is to resume. If this does not occur and the bus is left low for more than 16µs, one or more devices on the bus could be reset.

Transaction Sequence

The protocol for accessing the DS1964S through the 1-Wire port is as follows:

- Initialization
- ROM Function Command
- Memory/SHA Function Command
- Transaction Data

Initialization

All transactions on the 1-Wire bus begin with an initialization sequence. The initialization sequence consists of a reset pulse transmitted by the bus master followed by presence pulse(s) transmitted by the slave(s). The presence pulse lets the bus master know that the DS1964S is on the bus and is ready to operate. For more details, see the *1-Wire Signaling* section.

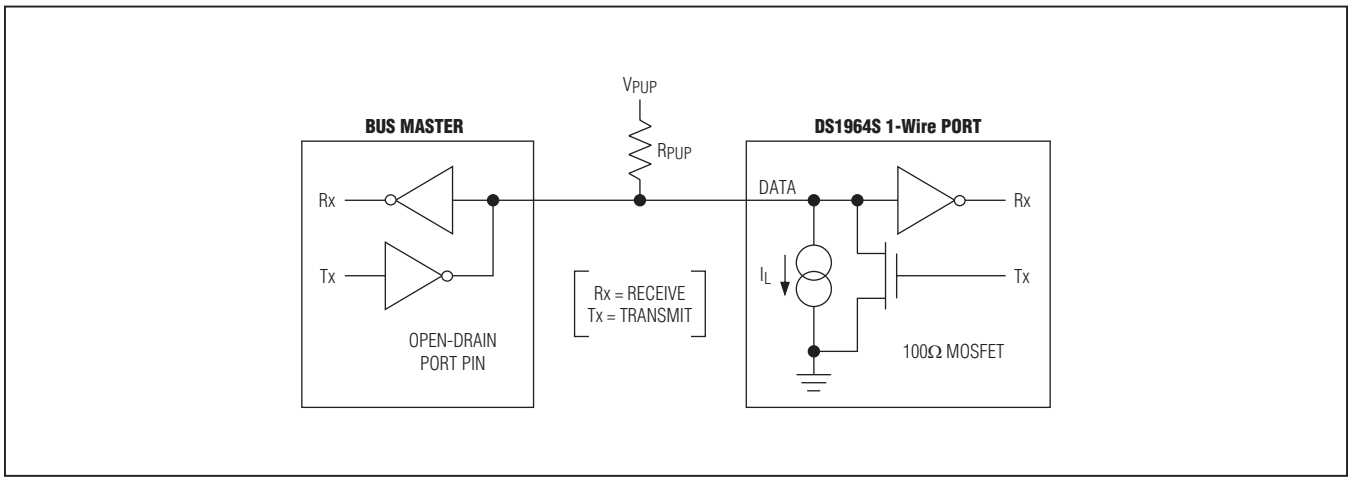


Figure 3. Hardware Configuration

1-Wire ROM Function Commands

Once the bus master has detected a presence, it can issue one of the five ROM function commands that the DS1964S supports. All ROM function commands are 8 bits long. A list of these commands follows (see the flowchart in Figure 4).

Read ROM [33h]

The Read ROM command allows the bus master to read the DS1964S's ROM ID (8-bit family code, unique 48-bit serial number, and 8-bit CRC). This command can only be used if there is a single slave on the bus. If more than one slave is present on the bus, a data collision occurs when all slaves try to transmit at the same time (open drain produces a wired-AND result).The family code and 48-bit serial number as read by the master are unlikely to match the CRC.

Match ROM [55h]

The Match ROM command, followed by a 64-bit ROM ID, allows the bus master to address a specific DS1964S on a multidrop bus. Only the DS1964S that exactly matches the 64-bit ROM ID responds to the following memory or SHA function command. All other slaves wait for a reset pulse. This command can be used with a single or multiple devices on the bus.

Search ROM [F0h]

When a system is initially brought up, the bus master might not know the number of devices on the 1-Wire bus or their ROM ID numbers. By taking advantage of the wired-AND property of the bus, the master can use a process of elimination to identify the ID of all slave devices. For each bit of the ID number, starting with the least significant bit, the bus master issues a triplet of time slots. On the first slot, each slave device participating in the search outputs the true value of its ID number bit. On the second slot, each slave device participating in the search outputs the complemented value of its ID number bit. On the third slot, the master writes the true value of the bit to be selected. All slave devices that do not match the bit written by the master stop participating in the search. If both of the read bits are zero, the master knows that slave devices exist with both states of the bit. By choosing which state to write, the bus master branches in the search tree. After one complete pass, the bus master knows the ROM ID number of a single device. Additional passes identify the ID numbers of the remaining devices. Refer to Application Note 187: *1-Wire Search Algorithm* for a detailed discussion, including an example.

Skip ROM [CCh]

This command can save time in a single-drop bus system by allowing the bus master to access the memory or SHA functions without providing the 64-bit ROM ID. If more than one slave is present on the bus and, for example, a read command is issued following the Skip ROM command, data collision occurs on the bus as multiple slaves transmit simultaneously (open-drain pulldowns produce a wired-AND result).

Resume Command [A5h]

To maximize the data throughput in a multidrop environment, the Resume command is available. This command checks the status of the RC bit and, if it is set, directly transfers control to the memory and SHA functions, similar to a Skip ROM command. The only way to set the RC bit is through successfully executing the Match ROM or Search ROM command. Once the RC bit is set, the device can repeatedly be accessed through the Resume command. Accessing another device on the bus clears the RC bit, preventing two or more devices from simultaneously responding to the Resume command.

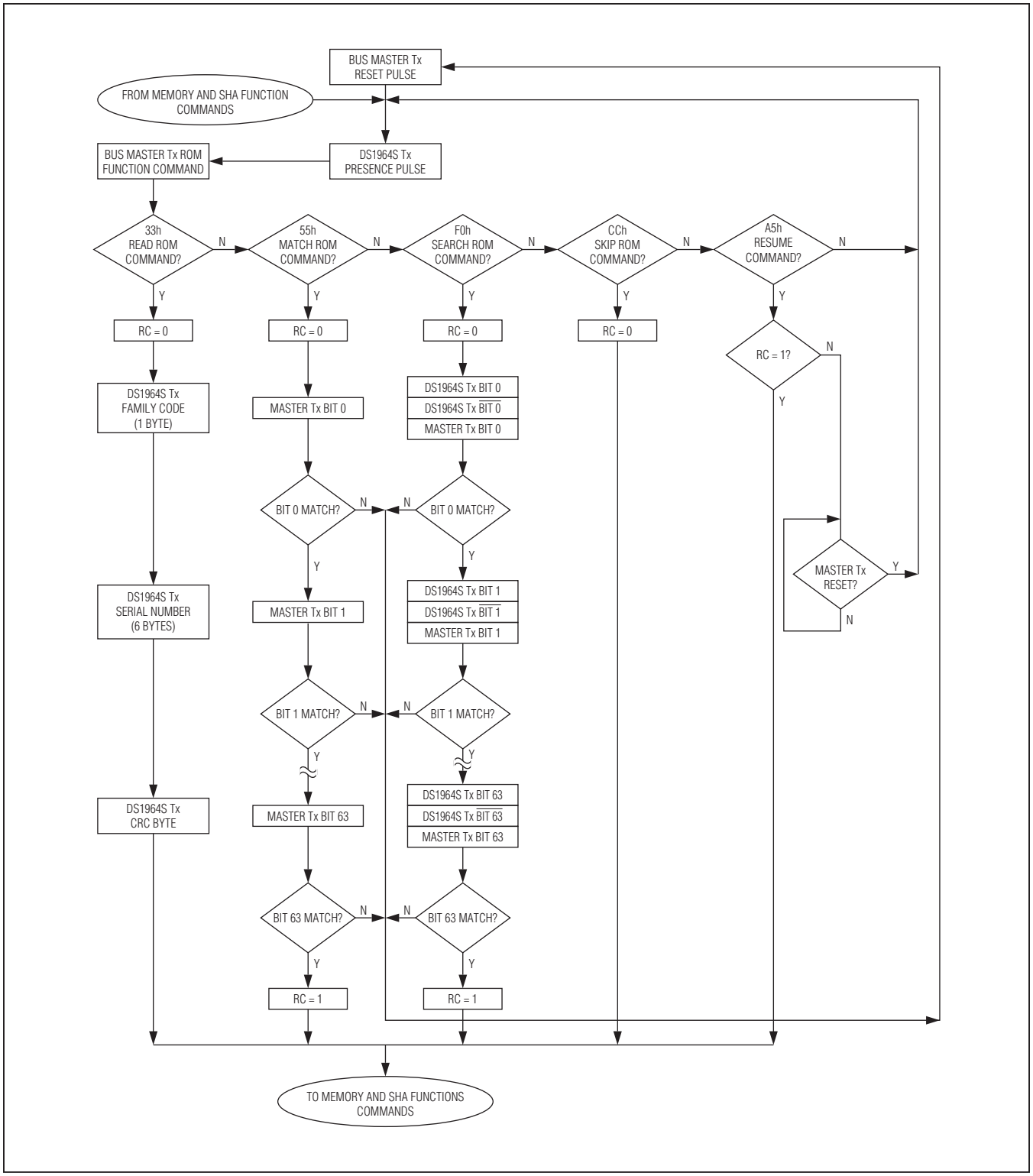


Figure 4. ROM Functions Flowchart (Refer to the Security Guide for Memory and SHA Function Commands Details)

1-Wire Signaling

The DS1964S requires strict protocols to ensure data integrity. The protocol consists of four types of signaling on one line: reset sequence with reset pulse and presence pulse, write-zero, write-one, and read-data. Except for the presence pulse, the bus master initiates all falling edges. The DS1964S communicates at overdrive speed only.

To get from idle to active, the voltage on the 1-Wire line needs to fall from V_{PUP} below the threshold V_{TL}. To get from active to idle, the voltage needs to rise from $V_{IL(MAX)}$ past the threshold V_{TH}. The time it takes for the voltage to make this rise is seen in Figure 5 as ε, and its duration depends on the pullup resistor (R_{PUP}) used and the capacitance of the 1-Wire network attached. The voltage $V_{IL(MAX)}$ is relevant for the DS1964S when determining a logical level, not triggering any events.

Figure 5 shows the initialization sequence required to begin any communication with the DS1964S. A reset pulse followed by a presence pulse indicates that the DS1964S is ready to receive data, given the correct ROM and memory and SHA function command. If the bus master uses slew-rate control on the falling edge, it must pull down the line for t_{RSTL} + t_F to compensate for the edge.

After the bus master has released the line it goes into receive mode. Now the 1-Wire bus is pulled to V_{PUP} through the pullup resistor. When the threshold V_{TH} is crossed, the DS1964S waits and then transmits a presence pulse by pulling the line low. To detect a presence pulse, the master must test the logical state of the 1-Wire line at t_{MSP}.

Read/Write Time Slots

Data communication with the DS1964S takes place in time slots that carry a single bit each. Write time slots transport data from bus master to slave. Read time slots transfer data from slave to master. Figure 6 illustrates the definitions of the write and read time slots.

All communication begins with the master pulling the data line low. As the voltage on the 1-Wire line falls below the threshold V_{TL}, the DS1964S starts its internal timing generator that determines when the data line is sampled during a write time slot and how long data is valid during a read time slot.

Master to Slave

For a **write-one** time slot, the voltage on the data line must have crossed the V_{TH} threshold before the write-one low time $t_{W1L(MAX)}$ is expired. For a **write-zero** time slot, the voltage on the data line must stay below the V_{TH} threshold until the write-zero low time $t_{W0L(MIN)}$ is expired. For the most reliable communication, the voltage on the data line should not exceed $V_{IL(MAX)}$ during the entire t_{W0L} or t_{W1L} window. After the V_{TH} threshold has been crossed, the DS1964S needs a recovery time t_{REC} before it is ready for the next time slot.

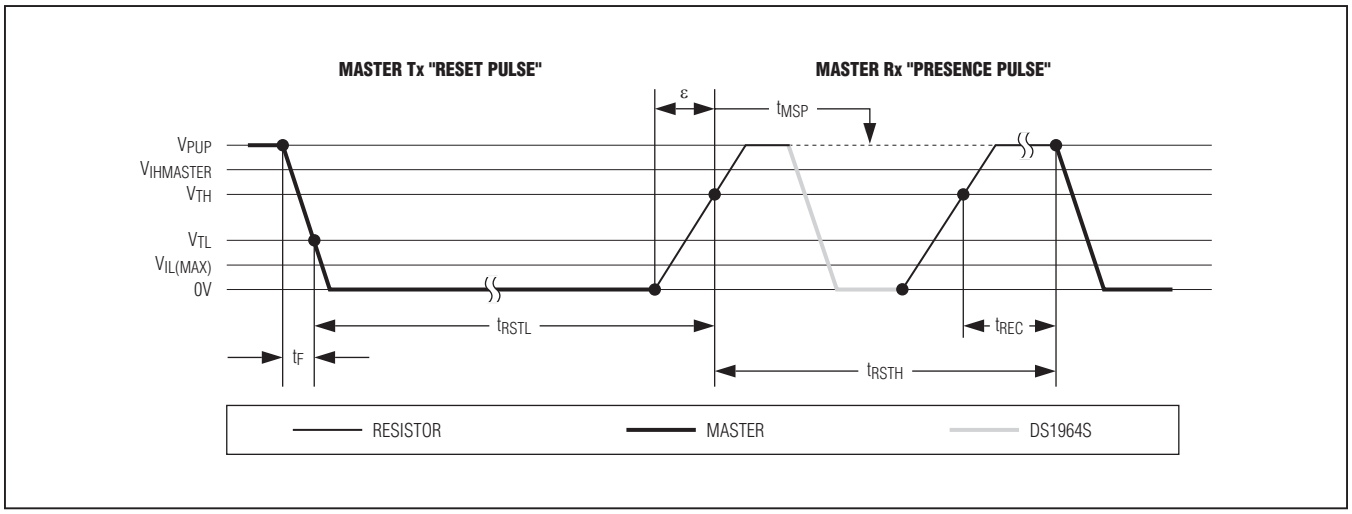


Figure 5. Initialization Procedure: Reset and Presence Pulse

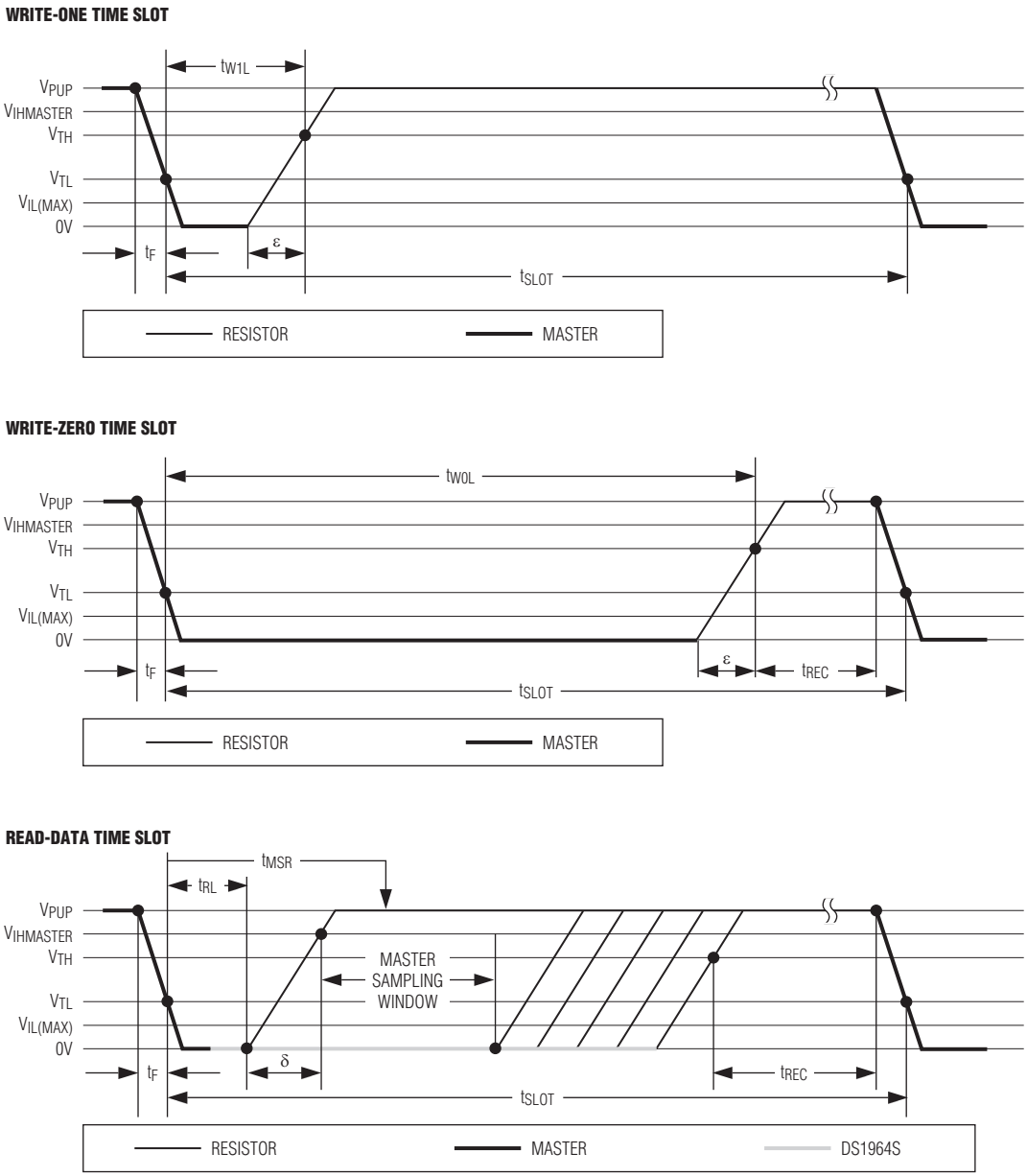


Figure 6. Read/Write Timing Diagrams

Slave to Master

A **read-data** time slot begins like a write-one time slot. The voltage on the data line must remain below V_{TL} until the read low time t_{RL} is expired. During the t_{RL} window, when responding with a 0, the DS1964S starts pulling the data line low; its internal timing generator determines when this pulldown ends and the voltage starts rising again. When responding with a 1, the DS1964S does not hold the data line low at all, and the voltage starts rising as soon as t_{RL} is over.

The sum of t_{RL} + δ (rise time) on one side and the internal timing generator of the DS1964S on the other side define the master sampling window ($t_{MSR(MIN)}$ to $t_{MSR(MAX)}$), in which the master must perform a read from the data line. For the most reliable communication, t_{RL} should be as short as permissible, and the master should read close to but no later than $t_{MSR(MAX)}$. After reading from the data line, the master must wait until t_{SLOT} is expired. This guarantees sufficient recovery time t_{REC} for the DS1964S to get ready for the next time slot. Note that t_{REC} specified herein applies only to a single DS1964S attached to a 1-Wire line. For multidevice configurations, t_{REC} must be extended to accommodate the additional 1-Wire device input capacitance.

Improved Network Behavior (Switchpoint Hysteresis)

In a 1-Wire environment, line termination is possible only during transients controlled by the bus master (1-Wire driver). 1-Wire networks, therefore, are susceptible to noise of various origins. Depending on the physical size and topology of the network, reflections from end points and branch points can add up or cancel each other to some extent. Such reflections are visible as glitches or ringing on the 1-Wire communication line. Noise coupled onto the 1-Wire line from external sources can also result in signal glitching. A glitch during the rising edge of a time slot can cause a slave device to lose synchronization with the master and, consequently, result in a Search ROM command coming to a dead end or cause a device-specific function command to abort. The DS1964S uses a 1-Wire front-end with built-in hysteresis at the low-to-high switching threshold V_{TH}. If a negative glitch crosses V_{TH} but does not go below V_{TH} - V_{HY}, it is not recognized (Figure 7).

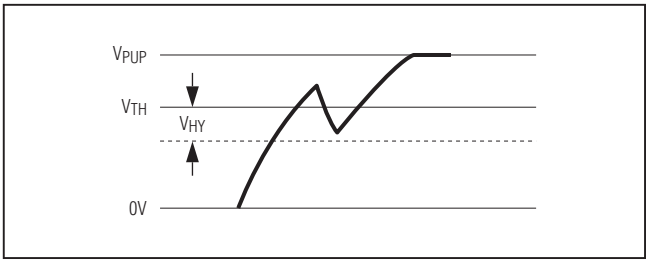


Figure 7. Noise Suppression Scheme

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS1964S-F5+	-40°C to +85°C	F5 iButton

+Denotes a lead(Pb)-free/RoHS-compliant package..

Package Information

For the latest package outline information and land patterns (footprints), go to **www.maximintegrated.com/packages**. Note that a "+", "#", or "-" in the package code indicates RoHS status only. Package drawings may show a different suffix character, but the drawing pertains to the package regardless of RoHS status.

PACKAGE TYPE	PACKAGE CODE	OUTLINE NO.
iButton F5 Can	IB+5NT	**21-0266**

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	6/18	Initial release	—

