DS2704

1280-Bit EEPROM with SHA-1 Authentication

www.maxim-ic.com

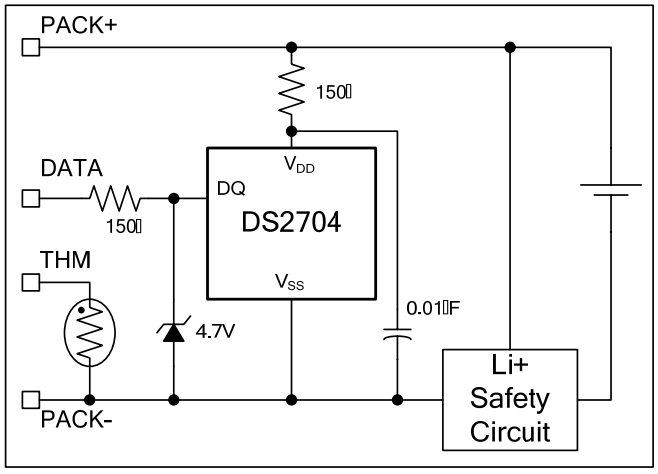
GENERAL DESCRIPTION

The DS2704 provides 1280 bits of EEPROM data storage and a Secure Hash Algorithm (SHA) engine. The Dallas 1-Wire® interface enables serial communication on a single battery contact and the 64-bit unique serial number allows multidrop networking and identification of individual devices.

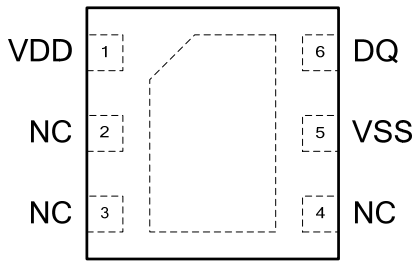
The 1280-bit memory is organized as 5 pages of 32 bytes each and supports storage of battery cell characteristics, charging voltage, current, and temperature parameters, as well as battery pack manufacturing data. The EEPROM pages are in circuit rewritable and can be individually locked to write protect data.

The DS2704 employs the Secure Hash Algorithm (SHA-1) specified in the Federal Information publication 180-1 and 180-2, and ISO/IEC 10118-3. SHA-1 provides a robust cryptographic solution to ensure battery packs or other peripherals have been manufactured by authorized sources. The DS2704 processes a host transmitted challenge and the 64-bit secret key stored on chip to produce a 160-bit response for transmission back to the host. The secret key is never transmitted between the battery and the host.

APPLICATION EXAMPLE



PIN CONFIGURATION



3mm × 3mm TDFN
(TOP VIEW—PADS ON BOTTOM)

APPLICATIONS

2.5G/3G Wireless Handsets
PDAs
Handheld or Notebook Computers and Terminals
Digital Still and Video Cameras

FEATURES

- Secure Challenge and Response Authentication Using the SHA-1 Algorithm
- Five Lockable 32-Byte Pages of EEPROM
- Dallas 1-Wire Interface with Standard and Overdrive Communications Speeds
- Unique 64-Bit Serial Number
- Compatible with DS2502 Memory Map and Read Function Command
- Operates with V_{DD} as Low as 2.5V
- Tiny Chip-Scale UCSP and 3mm x 3mm TDFN Packaging (Pb-Free)

ORDERING INFORMATION

PART	TEMP RANGE	PIN-PACKAGE
DS2704G+	-30°C to +85°C	3mm x 3mm TDFN-6
DS2704G+T&R	-30°C to +85°C	DS2704G+ on Tape-and-Reel
DS2704W	-30°C to +85°C	Bare Die

+ Denotes lead-free package.
1-Wire is a registered trademark of Dallas Semiconductor.

ABSOLUTE MAXIMUM RATINGS

Voltage Range on All Pins, Relative to V_{SS}	-0.3V to +6V
Operating Temperature Range	-40°C to +85°C
Storage Temperature Range	-55°C to +125°C
Soldering Temperature	See IPC/JEDEC J-STD-020A Specification

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 the absolute maximum rating conditions for extended periods may affect device.

RECOMMENDED DC OPERATING CONDITIONS

($2.5V \le V_{DD} \le 5.5V$, T_A = -30°C to +85°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{DD}	(Note 1)	2.5		5.5	V
Data Pin	DQ	(Note 1)	-0.3		+5.5	V

DC ELECTRICAL CHARACTERISTICS

($2.5V \le V_{DD} \le 5.5V$, T_A = -30°C to +85°C, typical values at V_{DD} = 3.7V and T_A = 25°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Active Current	I_{DD0}	Standby mode (Note 4)		1	3	µA
		-30°C ≤ T_A ≤ 70°C Standby mode (Note 4)		1	2	µA
	I_{DD1}	Communication mode using Standard Bus Timing (Note 5)		5	25	µA
		Communication mode using Overdrive Bus Timing (Note 5)		25	75	µA
	I_{DD2}	Computation mode		75	500	µA
	I_{DDP}	Programming mode		400	750	µA
Input Logic High: DQ	V_{IH}	(Note 1)	1.5			V
Input Logic Low: DQ	V_{IL}	(Note 1)			0.6	V
Output Logic Low: DQ	V_{OL}	I_{OL} = 4mA (Note 1)			0.4	V
Pull-down Current: DQ	I_{PD}			1	3	µA

EEPROM RELIABILITY SPECIFICATION

($2.5V \le V_{DD} \le 5.5V$, T_A = -30°C to +85°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Write Endurance: EEPROM Data Field	N_{EEC1}	(Note 2)	50,000			Writes
Write Endurance: Secret EEPROM	N_{EEC2}	(Note 2)	1,000			Writes
Storage	t_{EES}	(Note 2, 3)	10			Years

AC ELECTRICAL CHARACTERISTICS

($2.5V \le V_{DD} \le 5.5V$, T_A = -30°C to +85°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Computation Time	t_{SHA}				30	ms
EEPROM Copy Time	t_{EEC}	(Note 2)			10	ms

AC ELECTRICAL CHARACTERISTICS: 1-WIRE INTERFACE

(2.5V ≤ V_{DD} ≤ 5.5V, T_A = -30°C to +85°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
STANDARD BUS TIMING						
Time Slot	t_{SLOT}		60		120	µs
Recovery Time	t_{REC}		1			µs
Write 0 Low Time	t_{LOW0}		60		120	µs
Write 1 Low Time	t_{LOW1}		1		15	µs
Read Data Valid	t_{RDV}				15	µs
Reset Time High	t_{RSTH}		480			µs
Reset Time Low	t_{RSTL}		480		960	µs
Presence Detect High	t_{PDH}		15		60	µs
Presence Detect Low	t_{PDL}		60		240	µs
OVERDRIVE BUS TIMING						
Time Slot	t_{SLOT}		6		16	µs
Recovery Time	t_{REC}		1			µs
Write 0 Low Time	t_{LOW0}		6		16	µs
Write 1 Low Time	t_{LOW1}		1		2	µs
Read Data Valid	t_{RDV}				2	µs
Reset Time High	t_{RSTH}		48			µs
Reset Time Low	t_{RSTL}		48		80	µs
Presence Detect High	t_{PDH}		2		6	µs
Presence Detect Low	t_{PDL}		8		24	µs
DQ Capacitance	C_{DQ}				60	pF

Note 1: All voltages are referenced to V_{SS}.

Note 2: EEPROM programming temperature range limited to 0°C to 50°C.

Note 3: Device written N_{EEC} times then stored for t_{EES} at 50°C.

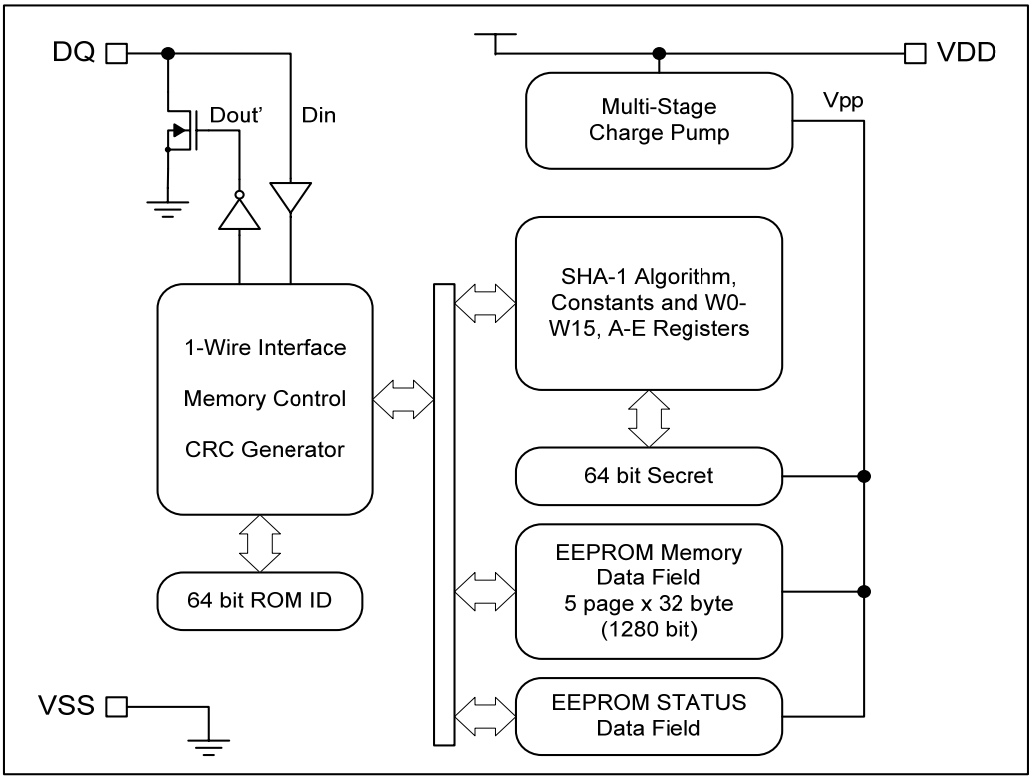
Note 4: DQ = V_{DD}.

Note 5: Current measured with minimum bus timing while the master issues: 1-Wire Reset, Skip ROM, Write Challenge, Write Repeated 0's until end of measurement.

PIN DESCRIPTION

PIN	SYMBOL	FUNCTION
6	DQ	Serial interface data I/O pin. Bi-directional data transmit and receive at 16kbps or 143kbps.
5	V_{SS}	Supply GND and reference for serial communication. Attach V_{SS} to battery pack negative terminal.
1	V_{DD}	Supply input. Bypass to V_{SS} with 0.01µF typical.
2, 3, 4	NC	No Connection

Figure 1. Block Diagram



DETAILED DESCRIPTION

The DS2704 is comprised of an EEPROM memory array and SHA-1 Authentication function that are accessed via a 1-Wire interface. The 1-Wire interface controls access by a host system to the 64-bit Net Address (ROM ID), SHA-1 Authentication, 1280-bit EEPROM memory and EEPROM Status.

The DS2704 operates in one of four modes: standby, communication, computation and programming. Standby mode is the default mode of operation. Whenever any task has been completed, the IC will automatically return to standby mode. Standby mode is also directly entered if DQ is low for a period of t_{RSTL}. Once standby mode has been entered, DQ can be returned to logic high and standby mode is retained. Most operations are performed in communication mode, with the host system addressing the DS2704 using Net Address commands and then retrieving EEPROM and Status data using memory function commands or setting up an authentication exchange and retrieving the results. The supply current, I_{DD1}, varies depending on bus activity, communication direction, and selection of Standard or Overdrive bus timing.

In SHA-1 computation mode, the supply current increases to I_{DD2} for a period of t_{SHA}. The computation mode load current occurs after the last bit of one of the Compute MAC function commands is sent.

Programming mode is entered when writing the nonvolatile memory portions of the DS2704. The supply current increases to I_{DDP} for t_{EEC} when a Copy Scratchpad, Write Status, Compute Secret, Clear/Lock Secret or Clear/Set Overdrive Timing command is executed.

Functional compatibility has been maintained between the DS2502 and DS2704 at the Net Address/ROM Command and Function Command levels for reading the Memory and Status data fields. Since the DS2704 is based on EEPROM technology versus the EPROM technology used for the DS2502, writing of the Memory and Status data fields is not the same as the DS2502. The DS2704 includes an on-chip charge pump to facilitate in-circuit programming. The need to apply an external high voltage programming pulse during pack manufacture is therefore eliminated. Data can be written to a 0 or 1 value up to N_{EEC} times in the DS2704. The ability to reprogram the data in the EEPROM pages makes the Page Address Redirection bytes in the Status data field unnecessary. Therefore, the DS2704 maintains them for DS2502 read compatibility but they cannot be modified from their factory default values of FFh.

AUTHENTICATION

Authentication is performed using a FIPS-180 compliant SHA-1 one way hash algorithm on a 512-bit message block. The message block consists of a 64-bit secret, a 64-bit challenge and 384 bits of constant data. Optionally, the 64-bit Net Address replaces 64 of the 384 bits of constant data used in the hash operation. Contact Dallas/Maxim for details of the message block organization.

The host and the DS2704 both calculate the result based on the mutually known secret. The result data, known as the Message Authentication Code (MAC) or Message Digest, is returned by the DS2704 for comparison to the host's result. Note that the secret is never transmitted on the bus and thus cannot be captured by observing bus traffic. Each authentication attempt is initiated by the host system by providing a 64-bit random challenge via the Write Challenge command. The host then issues the Compute MAC or Compute MAC with ROM ID command. The MAC is computed per FIPS 180, and then returned as a 160-bit serial stream, beginning with the least significant bit.

DS2704 AUTHENTICATION COMMANDS

WRITE CHALLENGE [0Ch]. This command writes the 64-bit challenge to the DS2704. The LSB of the 64-bit data argument can begin immediately after the MSB of the command has been completed. If more than 8 bytes are written, the final value in the challenge register will be indeterminate. The Write Challenge command **must be issued prior to every** Compute MAC or Compute Next Secret command for reliable results.

COMPUTE MAC WITHOUT ROM ID [36h]. This command initiates a SHA-1 computation based on the Challenge Value and Internal Secret. Logical 1's are loaded in place of the ROM ID. This command allows the use of a master secret and MAC response independent of the ROM ID. The DS2704 computes the MAC in t_{SHA} after receiving the last bit of this command. After the MAC computation is complete, the host must write 8 write zero time slots and then issue 160 read time slots to receive the 20-byte MAC. See Figure 7 on page 18 for command timing.

COMPUTE MAC WITH ROM ID [35h]. This command is structured the same as the Compute MAC without ROM ID, except that the ROM ID is included in the message block. With the ROM ID unique to each DS2704 included in the MAC computation, use of a unique secret in each token and a master secret in the host device is allowed. See application note "White Paper 4", available at http://www.maxim-ic.com, for more information. See Figure 7 on page 18 for command timing.

***NOTE**: Immediately after power-up, a dummy Compute MAC command is required to initialize the DS2704. If the dummy command is not issued, the first authentication attempt is computed using a challenge value of 0. When issuing the dummy Compute MAC command, the command sequence can be terminated immediately following the 8th bit of the Compute MAC command byte. Waiting for the SHA-1 computation and reading the results back are not required.*

SHA-1 related commands used while authenticating a battery or peripheral device are summarized in Table 1 for convenience. Four additional commands for clearing, computing and locking of the Secret are described in detail in the following section.

Table 1. Authentication Function Commands

COMMAND	HEX	FUNCTION
Write Challenge	0C	Writes 64-bit challenge for SHA-1 processing. Required prior to issuing Compute MAC and Compute Next Secret commands.
Compute MAC *without* ROM ID and return MAC	36	Computes hash the message block with logical 1's in place of the ROM ID. Returns the 160-bit MAC.
Compute MAC *with* ROM ID and return MAC	35	Computes hash of the message block including the ROM ID. Returns the 160-bit MAC.

SECRET MANAGEMENT FUNCTION COMMANDS

CLEAR SECRET [5Ah]. This command sets the 64-bit secret to all 0's (0000 0000 0000 0000h). The host must wait t_{EEC} for the DS2704 to write the new secret value to EEPROM. See Figure 10 on page 20 for command timing.

COMPUTE NEXT SECRET WITHOUT ROM ID [30h]. This command initiates a SHA-1 computation of the MAC and uses a portion of the resulting MAC as the next or new secret. The MAC computation is performed with the current 64-bit secret and the 64-bit challenge. Logical 1's are loaded in place of the ROM ID. 64-bits of the output MAC are used as the new secret value. The host must allow t_{SHA} after issuing this command for the SHA calculation to complete, then wait t_{EEC} for the DS2704 to write the new secret value to EEPROM. See Figure 8 on page 19 for command timing.

COMPUTE NEXT SECRET WITH ROM ID [33h]. This command initiates a SHA-1 computation of the MAC and uses a portion of the resulting MAC as the next or new secret. The MAC computation is performed with the current 64-bit secret, the 64-bit ROM ID and the 64-bit challenge. 64-bits of the output MAC are used as the new secret value. The host must allow t_{SHA} after issuing this command for the SHA calculation to complete, then wait t_{EEC} for the DS2704 to write the new secret value to EEPROM. See Figure 8 on page 19 for command timing.

LOCK SECRET [6Ah]. This command write protects the 64-bit Secret to prevent accidental or malicious overwrite of the secret value. The Secret value stored in EEPROM becomes "final." The host must wait t_{EEC} for the DS2704 to write the lock secret bit to EEPROM. See Figure 10 on page 20 for command timing.

Table 2. Secret Loading Function Commands

COMMAND	HEX	FUNCTION
Clear Secret	5A	Clears the 64-bit Secret to 0000 0000 0000 0000h
Compute Next Secret *without* ROM ID	30	Generates new global secret
Compute Next Secret *with* ROM ID	33	Generates new unique secret
Lock Secret	6A	Sets lock bit to prevent changes to the Secret

1-WIRE SPEED CONTROL FUNCTION COMMANDS

CLEAR OVERDRIVE [8Dh]. This command selects the Standard 1-Wire timings shown in the Electrical Characteristics table. The setting is stored in EEPROM so that the programmed speed selection can be recalled on initial power up. The host must wait t_{EEC} for the DS2704 to write the EEPROM. See Figure 10 for command timing. Standard 1-Wire timing is the factory default.

SET OVERDRIVE [8Bh]. This command selects the Overdrive 1-Wire timings shown in the Electrical Characteristics table. The setting is stored in EEPROM so that the programmed speed selection can be recalled on initial power up. The host must wait t_{EEC} for the DS2704 to write the EEPROM. See Figure 10 for command timing.

Table 3. 1-Wire Speed Control Function Commands

COMMAND	Hex	FUNCTION
Set Overdrive	8B	Sets 1-Wire interface timings to OVERDRIVE.
Clear Overdrive	8D	Sets 1-Wire interface timings to STANDARD. (Factory Default)

EEPROM MEMORY

The DS2704 has a linear address space for access to the EEPROM data field. The Read Memory and Read Data/Generate CRC Memory function commands provide DS2502 legacy read access to the lower 1024 bits of the EEPROM data field. Read access to the entire EEPROM data field is provided by the Read All function command. The Write Scratchpad, Read Scratchpad and Copy Scratchpad function commands provide write access to the EEPROM data field. The EEPROM memory is organized as 5 pages of 32 bytes each as shown in Table 4. EEPROM Data Field. All pages are read and write (R/W) accessible. When received from the factory, the entire 1280-bit EEPROM data field appears as logical 1's.

Table 4. EEPROM Data Field

ADDRESS (HEX)	DESCRIPTION	READ/WRITE
0000 – 001F	PAGE 0 (32 bytes)	R/W*
0020 – 003F	PAGE 1 (32 bytes)	R/W*
0040 – 005F	PAGE 2 (32 bytes)	R/W*
0060 – 007F	PAGE 3 (32 bytes)	R/W*
0080 – 009F	PAGE 4 (32 bytes)	R/W*
00A0 – FFFF	Reserved	

* *Writing requires programming delay of* t_{EEC}

READ MEMORY [F0h]. The Read Memory command is used to read data from the lower 1024 bits (PAGE 0 to PAGE 3) of the 1280-bit EEPROM data field. The bus master follows the command byte with a 2-byte address (TA1=(T7:T0), TA2=(T15:T8)) that indicates a starting byte location within the data field. An 8-bit CRC of the command byte and address bytes is computed by the DS2704 and read back by the bus master to confirm that the correct command word and starting address were received. If the CRC is deemed to be incorrect by the bus master, a reset pulse should be issued and the entire sequence repeated. If the CRC is deemed to be correct by the bus master, read time slots can be issued to receive data from the EEPROM data field starting at the initial address. The bus master can issue a reset pulse at any point or continue to issue read time slots until the end of PAGE 3 of the data field is reached.

If reading continues through the end of PAGE 3, the bus master can issue eight additional read time slots and the DS2704 will respond with a 8-bit CRC of all data bytes read from the initial starting byte through the last byte of PAGE 3. Terminating the command transaction with a reset pulse prior to reaching the end of PAGE 3 results in a loss of availability of the 8-bit CRC.

READ DATA/GENERATE 8-BIT CRC [C3h]

The Read Data/Generate 8-bit CRC command is used to read data from the lower 1024 bits (PAGE 0 to PAGE 3) of the 1280-bit EEPROM data field. The bus master follows the command byte with a 2-byte address (TA1=(T7:T0), TA2=(T15:T8)) that indicates a starting byte location within the data field. An 8-bit CRC of the command byte and address bytes is computed by the DS2704 and read back by the bus master to confirm that the correct command word and starting address were received. If the CRC is deemed to be incorrect by the bus master, a reset pulse should be issued and the entire sequence repeated. If the CRC is deemed to be correct by the bus master, read time slots can be issued to receive data from the EEPROM data field starting at the initial address. The bus master can issue a reset pulse at any point or continue to issue read time slots until the end of

the 32-byte page is reached. If reading occurs through the end of the 32-byte page, the bus master can issue eight additional read time slots and the DS2704 will respond with a 8-bit CRC of all data bytes read from the initial starting byte through the last byte of the current page. After the CRC is received, additional read time slots return data starting with the first byte of the next page. This sequence will continue until the bus master reads PAGE 3 and its accompanying CRC. Thus each page of data can be considered to be 33 bytes long: the 32 bytes of user-programmed EEPROM data and an 8-bit CRC that gets generated automatically at the end of each page. The Read Data/Generate 8-Bit CRC command sequence can be exited at any point by issuing a reset pulse.

READ ALL [65h]. The Read All command is used to read data from all 1280 bits (PAGE 0 – PAGE 4) of the EEPROM data field. This includes PAGE 0 – PAGE 3 which are accessible via the DS2502 Read Memory and Read Data/Gen CRC legacy commands and PAGE 4 which is only accessible using the Read All command.

The bus master follows the command byte with a 2-byte address (TA1=(T7:T0), TA2=(T15:T8)) that indicates a starting byte location within the data field. An 8-bit CRC of the command byte and address bytes is computed by the DS2704. The bus master must issue 8 read time slots to receive the CRC value, and then issue additional read time slots to receive data from the DS2704 starting at TA2:TA1.

When reading begins within the EEPROM data field (0000h – 009Fh) and continues past 009Fh, an 8-bit CRC of all data returned is computed by the DS2704 and returned following the last byte of the data field. If reading begins in the reserved range or time slots are issued after receiving the 8-bit CRC, the DS2704 returns logical 1's.

WRITE SCRATCHPAD [6Ch]. The Write Scratchpad command is used to write up to 8 bytes to the scratchpad buffer which is in turn used to program 1280-bit EEPROM data field via the Copy Scratchpad command. The bus master issues the Write Scratchpad function command followed by a 1-byte address argument that depicts the starting byte position in the scratchpad of the following byte stream to be written. The valid range for the address is 00h – 07h. The address is auto-incremented after each data byte is written. When the address is greater than 07h, no further bytes will be accepted. Incomplete bytes are not written to the scratchpad. The Write Scratchpad command fills the scratchpad LSByte first, so when fewer than 8 bytes are written, the upper bytes of the scratchpad buffer contain data from previous operations. Since the Copy Scratchpad command transfers the entire scratchpad to the EEPROM data field, incomplete writing of the scratchpad should be done with caution. If the master determines the scratchpad data is unsuitable to copy to the EEPROM, the entire write sequence (command and data) must be repeated after issuing a reset pulse.

READ SCRATCHPAD [69h]. The Read Scratchpad command is used to return scratchpad data if verification of the scratchpad data is required prior to programming the EEPROM data field. The bus master issues the Read Scratchpad function command followed by a 1-byte address argument that depicts the starting byte position in the scratchpad of the first byte to be read. The valid range for the address is 00h – 07h. The address is auto-incremented after each data byte is read. When the address is greater than 07h, any further reads will return bit values of 1. The DS2704 returns up to 64 bits from the scratchpad beginning with the least significant bit of the least significant byte.

COPY SCRATCHPAD [48h]. The Copy Scratchpad function command is used to transfer data from the 8-byte scratchpad buffer to the EEPROM data field memory. Transfers are aligned on 8-byte boundaries. The bus master issues the Copy Scratchpad function command followed by the 2-byte target address (TA1=(T7:T0), TA2=(T15:T8)). The DS2704 aligns target addresses to the least significant byte (LSByte) of each eight byte boundary by zeroing the three least significant bits of TA1. That is, TA1[T2:T0] are set internally to 000b. As an example, issuing the Copy Scratchpad command with TA2:TA1 = 0x0020 or TA2:TA1 = 0x0027 results in the same 8-byte block being copied to PAGE 1 beginning at address 0x0020.

A delay of t_{EEC} is required to program the scratchpad contents to the EEPROM array. See Figure 9 for command timing.

EEPROM STATUS

The DS2704 has a separate 8-byte linear address space for access to the EEPROM Status data field using the Read Status and Write Status Function Commands.

READ STATUS [AAh]. The Read Status command is used to read data from the EEPROM Status data field. The bus master follows the command byte with a 2-byte address (TA1=(T7:T0), TA2=(T15:T8)) that indicates a starting byte location within the data field. An 8-bit CRC of the command byte and address bytes is computed by the DS2704 and read back by the bus master to confirm that the correct command word and starting address were received. If the CRC is deemed to be incorrect by the bus master, a reset pulse should be issued and the entire sequence repeated. If the CRC is deemed to be correct by the bus master, read time slots can be issued to receive data starting at the initial address. The bus master can issue a reset pulse at any point or continue to issue read time slots until the end of the EEPROM Status data field is reached. If reading occurs through the end of the EEPROM Status data field, the bus master can issue eight additional read time slots and the DS2704 will respond with a 8-bit CRC of all data bytes read from the initial starting byte through the last byte. Additional read time slots return logical 1's. The Read Status command sequence can be ended at any point by issuing a reset pulse.

Table 5. EEPROM Status Field

ADDRESS (HEX)	DESCRIPTION	READ/WRITE
0000	Write Protect Page bits B0: Page 0 Write Protect B1: Page 1 Write Protect B2: Page 2 Write Protect B3: Page 3 Write Protect B4: Page 4 Write Protect B5: Reserved for TMEX B6: Reserved for TMEX B7: Reserved for TMEX	R/W*
0001	Factory Programmed to FFh	R
0002	Factory Programmed to FFh	R
0003	Factory Programmed to FFh	R
0004	Factory Programmed to FFh	R
0005-0006	Reserved	R
0007	Factory Programmed to 00h	R

**One time write to "0"*

WRITE STATUS [55h]

The Write Status command is used to program the EEPROM Status data field. Only the Write Protect Page bits at address 0000h are writable. The other bytes are factory programmed to the values in Table 5. The Write Protect Page bits are set to logical 1's when received from the factory. EEPROM page data can be programmed multiple times until its associated Write Protect Page bit is programmed to a logical 0. Once a Write Protect Page bit is programmed to a logical 0, it cannot be programmed back to a logical 1. Programming a Write Protect Page bit to a logical 0 prevents any future modification or overwriting of the data in the associated page.

To protect page data from modification, the bus master writes the Write Status function command followed by one byte of status data containing the Write Protect Page bits (B7:B0). The status data must be written least significant bit to most significant bit, that is B0 to B7. Once the eighth bit of the status data is completed, the write operation cannot be undone. If the write operation is abandoned prior to completing the status data byte, the entire write sequence must be repeated after issuing a reset pulse.

After the programming write delay (t_{EEC}), the master can issue a Read Status function command to verify that the appropriate Write Protect Page bits have been programmed.

Table 6. EEPROM Memory and Status Function Commands

COMMAND	HEX	FUNCTION
Read Memory	F0	Read data from the lower 1024 bits of the 1280-bit EEPROM Memory data field. Generates a CRC value if read continues to end of the 4th page.
Read Data/Generate CRC	C3	Read data from lower 4 pages of the EEPROM Memory data field. Generates a CRC value of the data read from each page if read continues to the end of page.
Read All	65	Read data from all 5 pages of the EEPROM Memory data field.
Read Status	AA	Read data from the 8-byte EEPROM Status data field.
Write Status	55	Write the Page Protection bits in the EEPROM Status data field.
Write Scratchpad	6C	Write up to 8 bytes of data to the Scratchpad register.
Read Scratchpad	69	Read up to 8 bytes of the Scratchpad register data.
Copy Scratchpad	48	Programs the Scratchpad data to EEPROM DATA FIELD at the target address TA2:TA1.

***Note**: The Read Data, Read Data/Generate CRC and Read Status commands filter the target address (TA2:TA1) value with a 007Fh AND mask that limits the addressable size of the EEPROM Data Field and EEPROM Status Field to 1024 bits. Target address values equal to or greater than 0080h (128 decimal) return data from the lower 128 bytes of the respective data field. It is also important to note that the filter is applied prior to calculation of the CRC, so that target address values that are multiples of 128 return the same CRC. The CRC values should be considered correct only for TA2:TA1 = 0000h to 007Fh.*

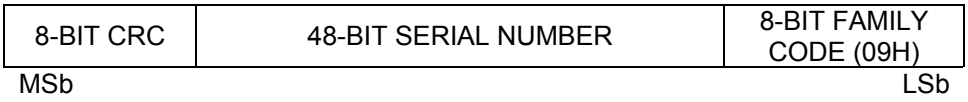
1-Wire BUS SYSTEM

The 1-Wire bus is a system that has a single bus master and one or more slaves. A multidrop bus is a 1-Wire bus with multiple slaves, while a single-drop bus has only one slave device. In all instances, the DS2704 is a slave device. The bus master is typically a microprocessor in the host system. The discussion of this bus system consists of five topics: 64-bit Net Address, CRC generation, hardware configuration, transaction sequence, and 1-Wire signaling.

64-BIT NET ADDRESS (ROM ID)

Each DS2704 has a unique, factory-programmed 1-Wire Net Address that is 64 bits in length. The term Net Address is synonymous with the ROM ID or ROM Code terms used in the DS2502 and other Dallas 1-Wire documentation. The first eight bits of the Net Address are the 1-Wire family code (09h). The next 48 bits are a unique serial number. The last eight bits are a cyclic redundancy check (CRC) of the first 56 bits (see Figure 2). The 64-bit Net Address and the 1-Wire I/O circuitry built into the device enable the DS2704 to communicate through the 1-Wire protocol detailed in this data sheet.

Figure 2. 1-Wire Net Address Format



CRC GENERATION

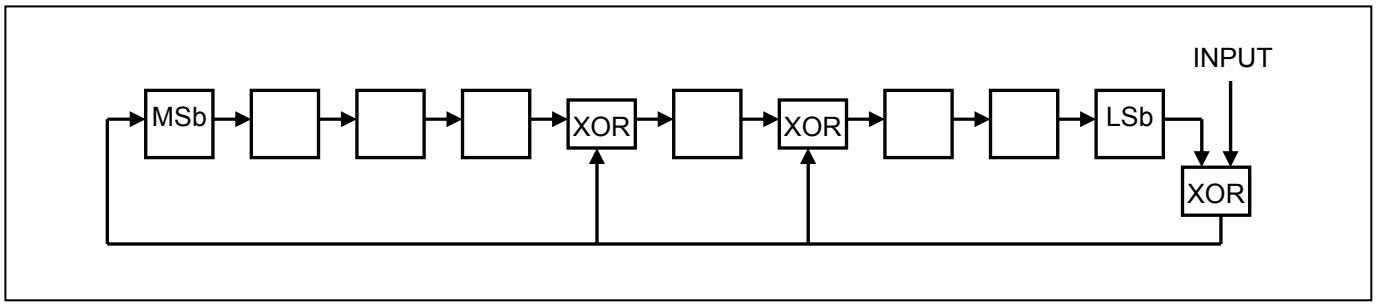
The DS2704 has an 8-bit CRC stored in the most significant byte of its 1-Wire net address and generates a CRC during some command protocols. To ensure error-free transmission of the address, the host system can compute a CRC value from the first 56 bits of the address and compare it to the CRC from the DS2704.

The host system is responsible for verifying the CRC value and taking action as a result. The DS2704 does not compare CRC values and does not prevent a command sequence from proceeding as a result of a CRC mismatch. Proper use of the CRC can result in a communication channel with a very high level of integrity.

The CRC can be generated by the host using a circuit consisting of a shift register and XOR gates as shown in Figure 3, or it can be generated in software using the polynomial $X^8 + X^5 + X^4 + 1$. Additional information about the Dallas 1-Wire CRC is available in *Application Note 27: Understanding and Using Cyclic Redundancy Checks with Dallas Semiconductor iButton® Products* (www.maxim-ic.com/appnoteindex).

In the circuit in Figure 3, the shift register bits are initialized to 0. Then, starting with the least significant bit of the family code, one bit at a time is shifted in. After the 8th bit of the family code has been entered, then the serial number is entered. After the 48th bit of the serial number has been entered, the shift register contains the CRC value.

Figure 3. 1-Wire CRC Generation Block Diagram



During some command sequences, the DS2704 also generates an 8-bit CRC and provides this value to the bus master to facilitate validation for the transfer of command, address, and data from the bus master to the DS2704. The DS2704 computes an 8-bit CRC for the command and address bytes received from the bus master for the Read Memory, Read Status and Read/Generate CRC commands to confirm that these bytes have been received correctly. The CRC generator on the DS2704 is also used to provide verification of error-free data transfer as each EEPROM page is sent to the master during a Read Data/Generate CRC command and for the 8 bytes of information in the Status memory field.

In each case where a CRC is used for data transfer validation, the bus master must calculate the CRC value using the same polynomial function and compare the calculated value to the CRC either stored in the DS2704 Net Address or computed by the DS2704. The comparison of CRC values and decision to continue with an operation are determined entirely by the bus master. There is no circuitry in the DS2704 that prevents the a command sequence from proceeding if the stored or calculated CRC from the DS2704 and the calculated CRC from the host do not match.

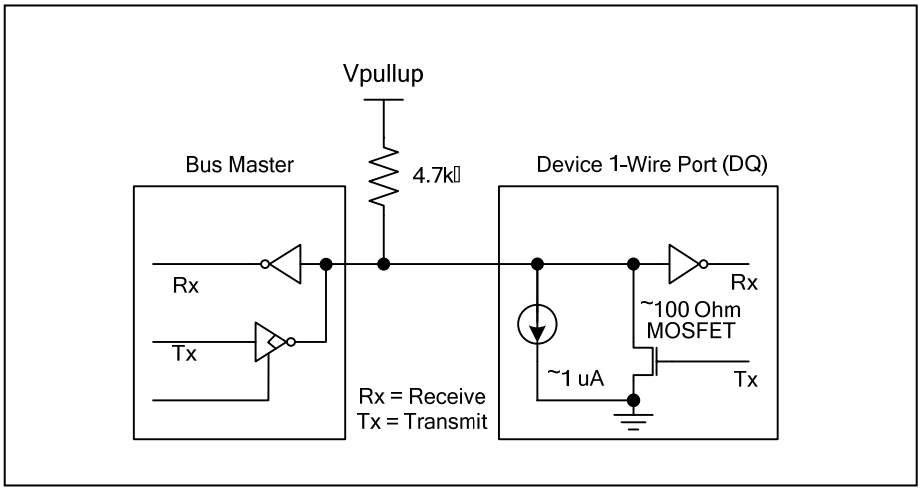
HARDWARE CONFIGURATION

Because the 1-Wire bus has only a single line, 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 connect to the bus with open-drain or tri-state output drivers. The DS2704 uses an open-drain output driver as part of the bidirectional interface circuitry shown in Figure 4. If a bidirectional pin is not available on the bus master, separate output and input pins can be connected together.

The 1-Wire bus must have a pullup resistor at the bus-master end of the bus. A value of between 2kΩ and 5kΩ is recommended. The idle state for the 1-Wire bus is high. If, for any reason, a bus transaction must be suspended, the bus must be left in the idle state to properly resume the transaction later. Note that if the bus is left low for more than t_{RSTL}, slave devices on the bus begin to interpret the low period as a reset pulse, effectively terminating the transaction.

iButton is a registered trademark of Dallas Semiconductor.

Figure 4. 1-Wire Bus Interface Circuitry



TRANSACTION SEQUENCE

The protocol for accessing the DS2704 through the 1-Wire port is as follows:

- Initialization
- Net Address Command
- Function Command(s)
- Data Transfer (not all commands have data transfer)

All transactions of the 1-Wire bus begin with an initialization sequence consisting of a reset pulse transmitted by the bus master, followed by a presence pulse simultaneously transmitted by the DS2704 and any other slaves on the bus. The presence pulse tells the bus master that one or more devices are on the bus and ready to operate. For more details, see the *I/O Signaling* section below.

NET ADDRESS COMMANDS

Once the bus master has detected the presence of one or more slaves, it can issue one of the net address commands described in the following paragraphs. The name of each Net Address command (ROM command) is followed by the 8-bit opcode for that command in square brackets.

Read Net Address [33h]. This command allows the bus master to read the DS2704's 1-Wire Net Address. This command can only be used if there is a single slave on the bus. If more than one slave is present, a data collision occurs when all slaves try to transmit at the same time (open drain produces a wired-AND result).

Match Net Address [55h]. This command allows the bus master to specifically address one DS2704 on the 1-Wire bus. Only the addressed DS2704 responds to any subsequent function command. All other slave devices ignore the function command and wait for a reset pulse. This command can be used with one or more slave devices on the bus.

Skip Net Address [CCh]. This command saves time when there is only one DS2704 on the bus by allowing the bus master to issue a function command without specifying the address of the slave. If more than one slave device is present on the bus, a subsequent function command can cause a data collision when all slaves transmit data at the same time.

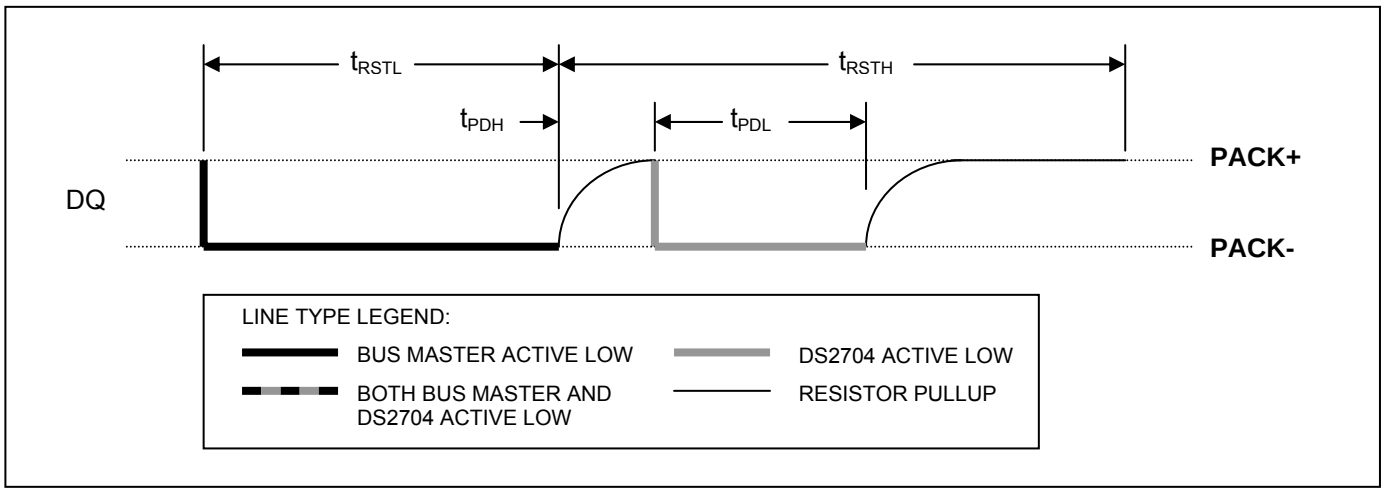
Search Net Address [F0h]. This command allows the bus master to use a process of elimination to identify the 1-Wire Net Addresses of all slave devices on the bus. The search process involves the repetition of a simple three-step routine: read a bit, read the complement of the bit, then write the desired value of that bit. The bus master performs this simple three-step routine on each bit location of the net address. After one complete pass through all 64 bits, the bus master knows the address of one device. The remaining devices can then be identified on additional iterations of the process. See Chapter 5 of the *Book of iButton Standards* for a comprehensive discussion of a Net Address search, including an actual example (www.maxim-ic.com/iButtonBook).

I/O SIGNALING

The 1-Wire bus requires strict signaling protocols to ensure data integrity. The four protocols used by the DS2704 are as follows: the initialization sequence (reset pulse followed by presence pulse), write 0, write 1, and read data. The bus master initiates all these types of signaling except the presence pulse.

The initialization sequence required to begin any communication with the DS2704 is shown in Figure 5. A presence pulse following a reset pulse indicates that the DS2704 is ready to accept a Net Address command. The bus master transmits (Tx) a reset pulse for t_{RSTL}. The bus master then releases the line and goes into receive mode (Rx). The 1-Wire bus line is then pulled high by the pullup resistor. After detecting the rising edge on the DQ pin, the DS2704 waits for t_{PDH} and then transmits the presence pulse for t_{PDL}.

Figure 5. 1-Wire Initialization Sequence



WRITE-TIME SLOTS

A write-time slot is initiated when the bus master pulls the 1-Wire bus from a logic-high (inactive) level to a logic-low level. There are two types of write-time slots: write 1 and write 0. All write-time slots must be t_{SLOT} in duration with a 1µs minimum recovery time, t_{REC}, between cycles. The DS2704 samples the 1-Wire bus line between t_{LOW1_MAX} and t_{LOW0_MIN} after the line falls. If the line is high when sampled, a write 1 occurs. If the line is low when sampled, a write 0 occurs. The sample window is illustrated in Figure 6. 1-Wire Write- and Read-Time Slots. For the bus master to generate a write 1 time slot, the bus line must be pulled low and then released, allowing the line to be pulled high less than t_{RDV} after the start of the write time slot. For the host to generate a write 0 time slot, the bus line must be pulled low and held low for the duration of the write-time slot.

READ-TIME SLOTS

A read-time slot is initiated when the bus master pulls the 1-Wire bus line from a logic-high level to a logic-low level. The bus master must keep the bus line low for at least 1µs and then release it to allow the DS2704 to present valid data. The bus master can then sample the data t_{RDV} from the start of the read-time slot. By the end of the read-time slot, the DS2704 releases the bus line and allows it to be pulled high by the external pullup resistor. All read-time slots must be t_{SLOT} in duration with a 1µs minimum recovery time, t_{REC}, between cycles. See Figure 6 and the timing specifications in the Electrical Characteristics table for more information.

Figure 6. 1-Wire Write- and Read-Time Slots

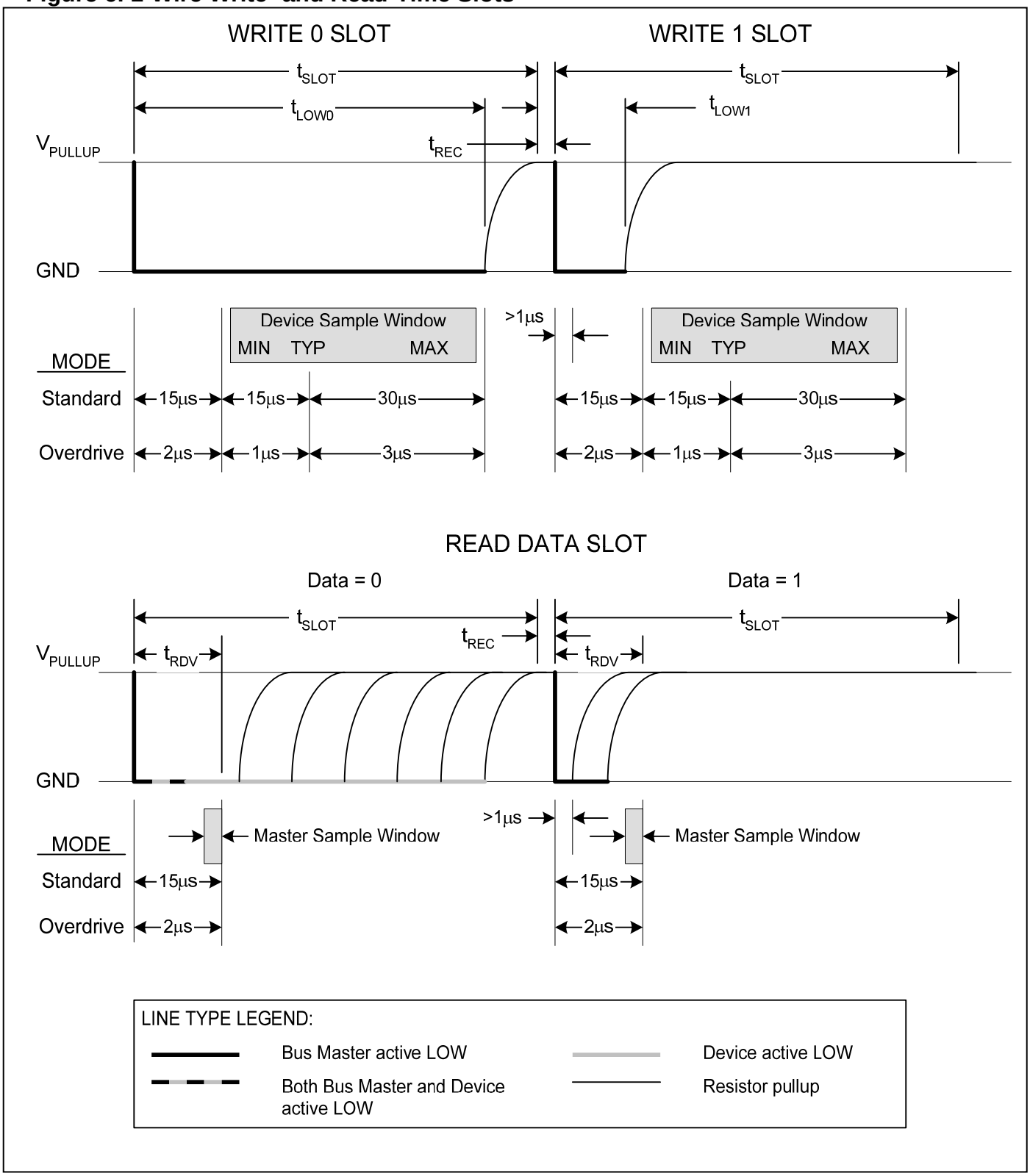


Table 7. All Function Commands

COMMAND	HEX	FUNCTION	COMPATIBILITY DS2502	COMPATIBILITY DS2703
Write Challenge	0C	Writes 64-bit challenge for SHA-1 processing. Required prior to all Compute MAC and Compute Next Secret commands.		**CC**
Compute MAC *without* ROM ID and return MAC	36	Computes hash of the message block with all 1's in place of the ROM ID.		**CC**
Compute MAC *with* ROM ID and return MAC	35	Computes hash of the message block using the ROM ID.		**CC**
Clear Secret	5A	Clears the 64-bit secret to 0000 0000 0000 0000h.		
Compute Next Secret *without* ROM ID	30	Generates new global secret.		**NP**
Compute Next Secret *with* ROM ID	33	Generates new unique secret.		**NP**
Lock Secret	6A	Sets lock bit to prevent changes to the Secret.		**NP**
Read Memory	F0	Read data from 1024-bit EEPROM Memory data field.	**CC**	
Read Data/Generate CRC	C3	Read data from 1024-bit EEPROM Memory data field and generate a CRC value of the data read during the operation.	**CC**	
Read All	65	Read data from the all 5 pages of the EEPROM Memory data field.		
Read Status	AA	Read data from the 8-byte EEPROM Status data field.	**CC**	
Write Status	55	Write data to the EEPROM Status data field.	**NP**	
Write Scratchpad	6C	Write data to the 8-byte Scratchpad buffer.		
Read Scratchpad	69	Read data from the 8-byte Scratchpad buffer.		
Copy Scratchpad	48	Write Scratchpad data to EEPROM data field.		
Set Overdrive	8B	Sets 1-Wire interface timings to OVERDRIVE.		**NP**
Clear Overdrive	8D	Sets 1-Wire interface timings to STANDARD. (Factory Default).		**NP**
Reset	BB	Resets DS2704 (Software POR).		**CC**

Key: CC—complete compatibility, NP—no programming pulse required on DS2704.

Table 8. Guide to Function Command Requirements

COMMAND	ISSUE MEMORY ADDRESS	ISSUE 00H BEFORE READ	READ/WRITE TIME SLOTS	READBACK CRC
Write Challenge			Write: 64	
Compute MAC		Yes	Read: up to 160	
Compute Next Secret				
Clear/Lock Secret, Set/Clear Overdrive				
Read Memory	16 bits: TA1, TA2		Read: up to 1024 (data) up to 16 (CRC)	After CMD + TA2:TA1, End of Page 3
Read Data/Gen CRC	16 bits: TA1, TA2		Read: up to 1024 (data) up to 40 (CRC)	After CMD + TA2:TA1, End of each page
Read All	16 bits: TA1, TA2		Read: up to 1280 (data)	After CMD + TA2:TA1, End of Page 4
Read Status	16 bits		Read: up to 64 (data) up to 16 (CRC)	After CMD + TA2:TA1, End of Status field
Write Status			Write: 8	
Write Scratchpad	8 bits		Write: up to 64	
Read Scratchpad	8 bits		Read: up to 64	
Copy Scratchpad	16 bits: TA1, TA2			
Reset				

Figure 7. Compute MAC Function Command

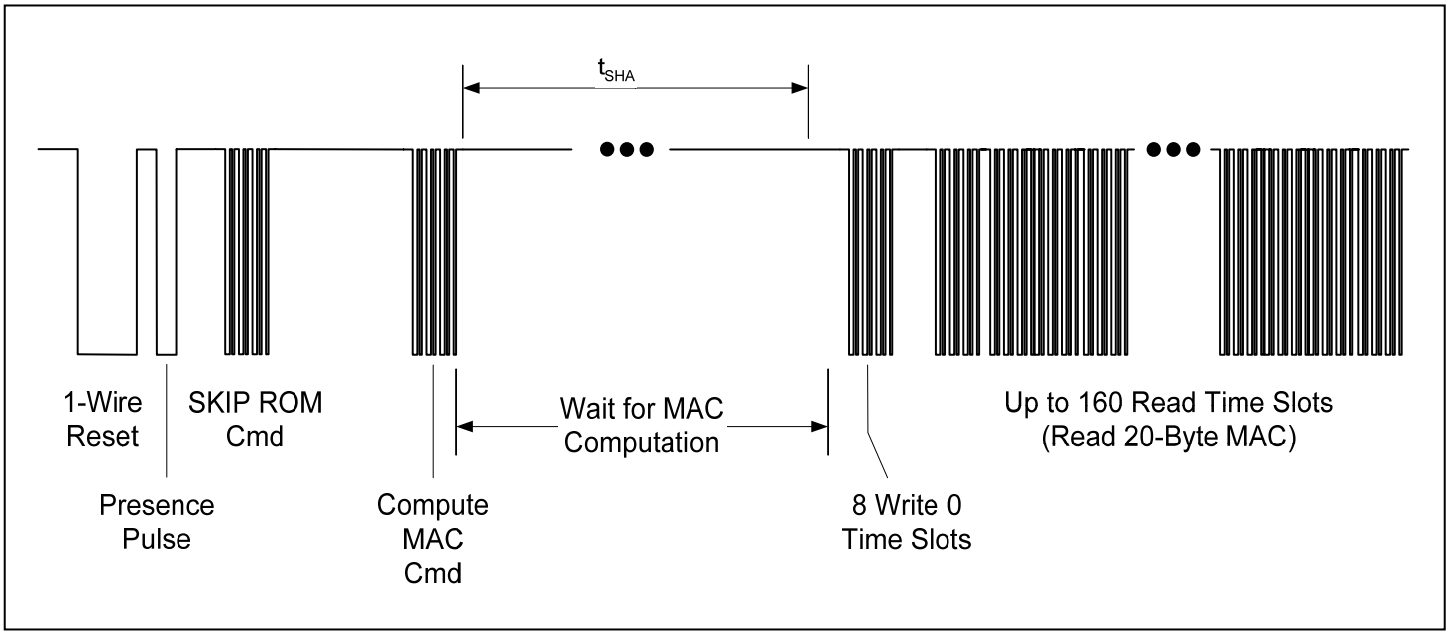


Figure 8. Compute Next Secret Function Command

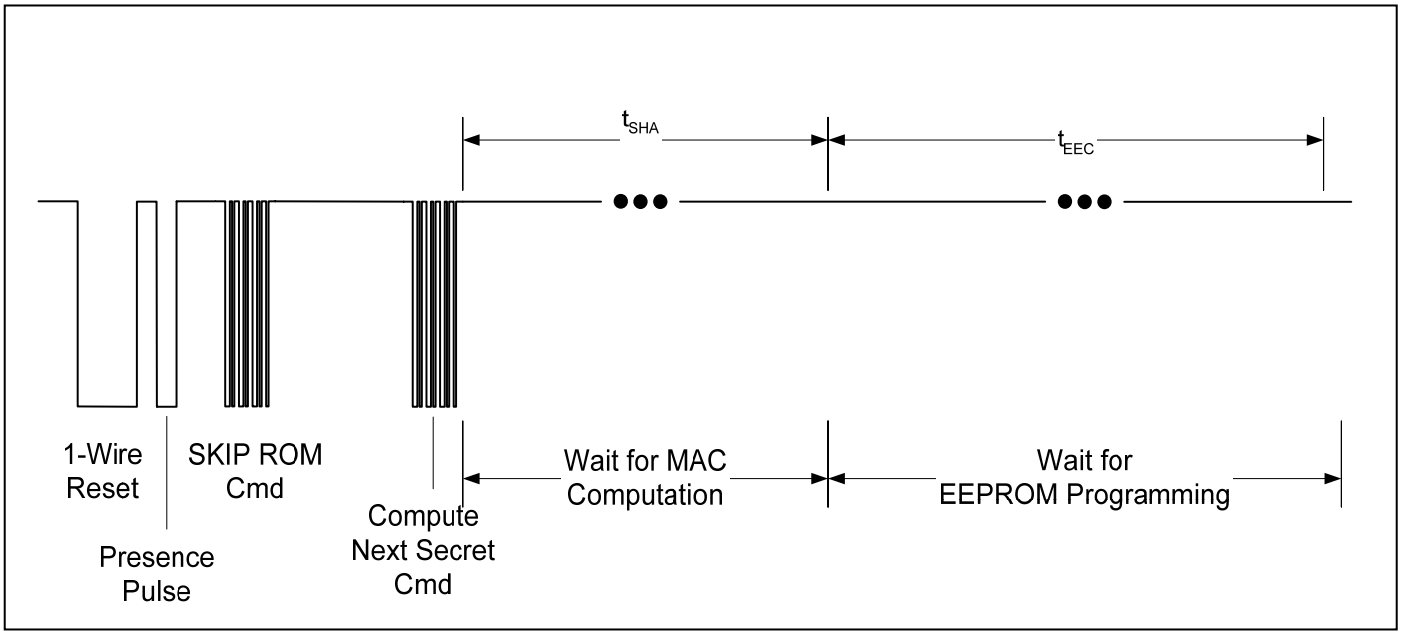


Figure 9. Copy Scratchpad Function Command

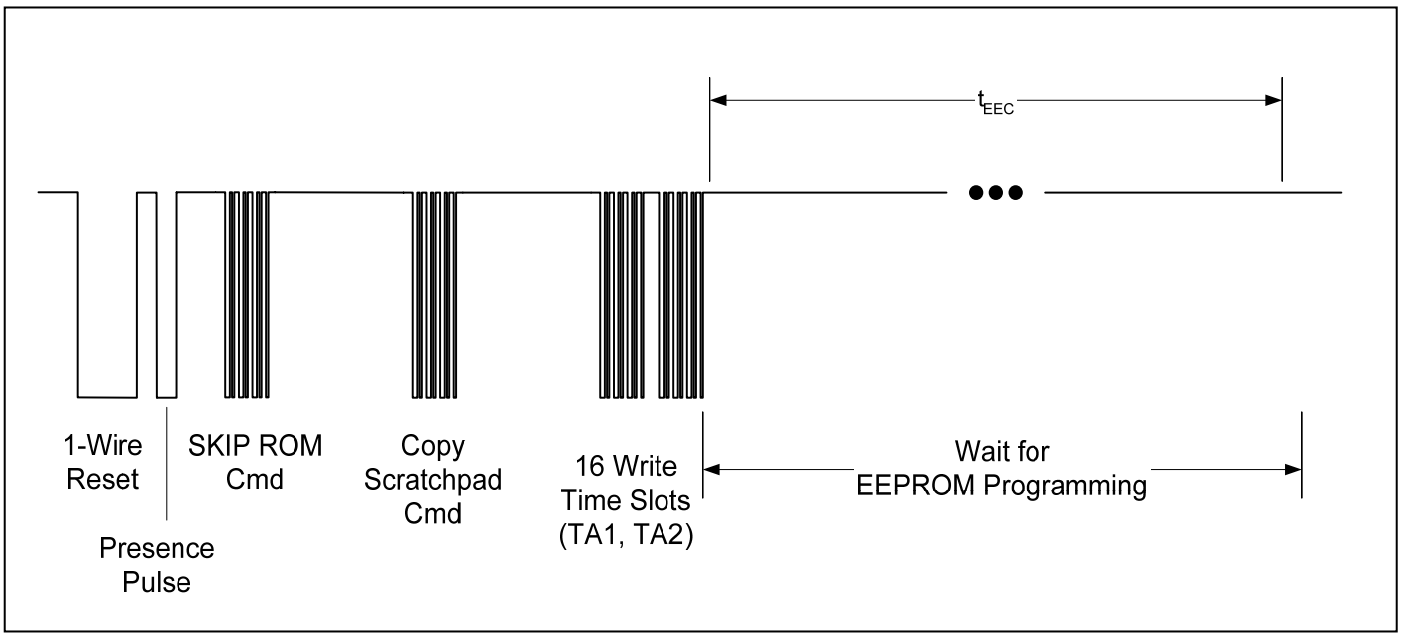
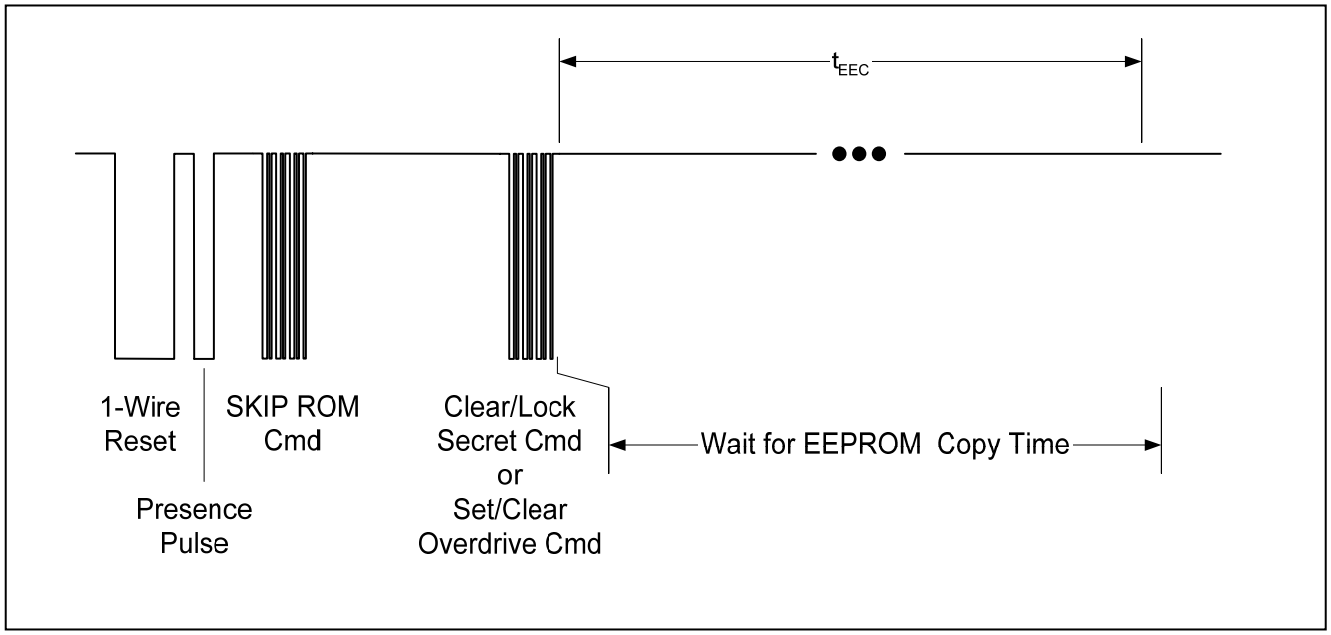


Figure 10. Clear/Lock Secret, Set/Clear Overdrive Function Commands



PACKAGE INFORMATION

(For the latest package outline information, go to **www.maxim-ic.com/DallasPackInfo**.)