DS2703
SHA-1 Battery Pack Authentication IC

www.maxim-ic.com

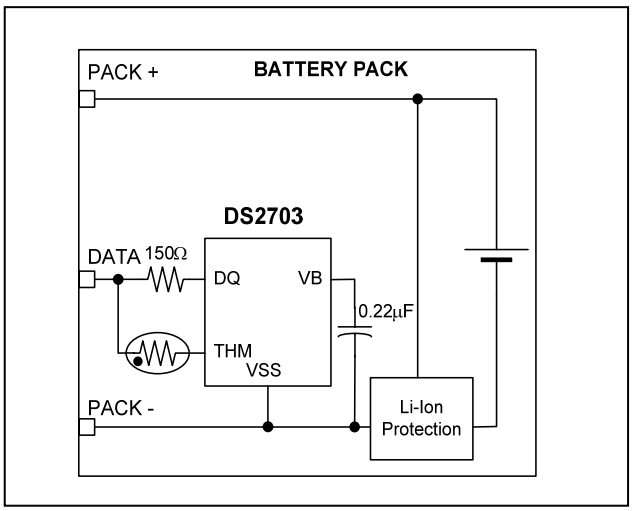
GENERAL DESCRIPTION

The DS2703 provides a robust cryptographic solution to ensure the authenticity of Li-Ion battery packs for cell phone, PDA, and portable computing devices. The DS2703 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 is designed for authentication—just what is required for identifying battery packs manufactured by authorized sources.

The device's SHA-1 engine processes a host transmitted challenge using its stored 64-bit secret key and unique 64-bit ROM ID to produce a 160-bit response word for transmission back to the host. The secret key is securely stored on-chip and never transmitted between the battery and the host. A DS2703-based system produces a high degree of authentication security between a host system and its removable battery or other peripheral devices.

The Thermistor Multiplexer feature allows a three contact battery pack configuration to support data and thermistor functions. When activated through 1-Wire command, the THM pin presents the thermistor impedance on the data contact and disconnects internal loading from the node.

TYPICAL OPERATING CIRCUIT

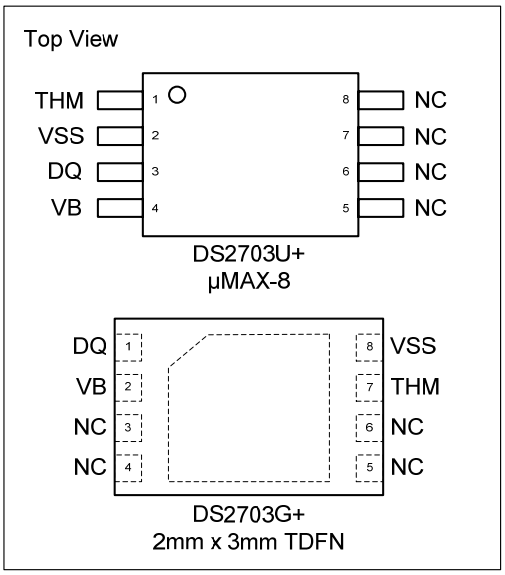


1-Wire is a registered trademark of Dallas Semiconductor.
µMAX is a registered trademark of Maxim Integrated Products.

FEATURES

- Secure Challenge and Response Authentication Using the SHA-1 Algorithm
- Directly Powered by the Dallas 1-Wire® Interface with 16kbps Standard and 143kbps Overdrive Communication Modes
- Unique 64-Bit Serial Number
- Thermistor Multiplexer
- Operates with V_{PULLUP} as Low as 2.7V
- Pb-Free 8-Pin µMAX® or 2mm x 3mm TDFN Package

PIN CONFIGURATION



APPLICATIONS

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

ORDERING INFORMATION

PART	TEMP RANGE	PIN-PACKAGE
DS2703G+	-20°C to +70°C	2mm x 3mm TDFN
DS2703G+T&R	-20°C to +70°C	DS2703G+ on Tape-and-Reel
DS2703U+	-20°C to +70°C	µMAX-8
DS2703U+T&R	-20°C to +70°C	DS2703U+ on Tape-and-Reel

+ Denotes lead-free package.

Note: *Some revisions of this device may incorporate deviations from published specifications known as errata. Multiple revisions of any device may be simultaneously available through various sales channels. For information about device errata, click here: www.maxim-ic.com/errata.*

REV: 061307

ABSOLUTE MAXIMUM RATINGS

Voltage Range on DQ, THM Pins Relative to Ground	-0.3V to +18V
Voltage Range on VB Pin Relative to Ground	-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

(T_A = -20°C to +70°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
DQ Pullup Voltage	V_{PULLUP}	Communication Mode	0		5.5	V
		Computation Mode	2.7		5.5	
DQ, THM Relative Voltage	V_{DQ-THM}	(Note 1)	-0.3		15	V
DQ to THM Resistor	R_{DQ-THM}	(Note 2)	5		500	KΩ

DC ELECTRICAL CHARACTERISTICS

(V_{PULLUP} = 2.7V to 5.5V, T_A = -20°C to +70°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
DQ Load Current	I_{DQ0}	Standby Mode, $V_{DQ} > V_{IH}$		1	2.5	µA
	I_{DQ1}	Communication Mode (Note 14)			75	µA
	I_{DQ2}	Computation Mode, SHA-1 Computation Active			0.25	mA
	I_{DQ3}	Thermistor Mux Active, (Note 3)			1	µA
	I_{PP}	$14.5 < V_{DQ} < 15.0V$ $0 < t < 50\ ^oC$			10	mA
	$I_{PP-IDLE}$	(Note 4)			60	µA
DQ Programming Voltage	V_{PP}	Program Pulse, (Note 5, 6)	14.5		15.0	V
Input Logic High: DQ	V_{IH}	(Note 6)	0.8 V_{PULLUP}			V
Input Logic Low: DQ	V_{IL}	(Note 6)			0.5	V
Output Logic Low: DQ	V_{OL-DQ}	I_{OL} = 4mA, (Note 6, 7)			0.4	V
Output Logic Low: THM	V_{OL-THM}	I_{OL} = 4mA, (Note 6, 7, 8)			0.4	V
Hold-Up Current: VB pin	I_{HU}	THM pin Active, V_B = 2.70V			3.2	µA
DQ Capacitance	C_{DQ}	(Note 9)		50		pF

EEPROM RELIABILITY SPECIFICATION

(V_{PULLUP} = 2.7V to 5.5V, T_A = -20°C to +70°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
EEPROM Write Endurance	N_{EEC}	$0 < t < 50\ ^oC$ (Note 10)	1000			Cycles

AC ELECTRICAL CHARACTERISTICS

(V_{PULLUP} = 2.7V to 5.5V, T_A = -20°C to +70°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
THM Low Delay	t_{TD}	(Note 11)			15	µs
Computation Delay Time	t_D	(Note 12)	100			µs
Computation Time	t_{SHA}	(Note 12)			15	ms
Programming Pulse Width	t_{PPW}	(Note 5)	17			ms
Programming Pulse Rise Time	t_{PPR}		0.5		5	µs
Programming Pulse Fall Time	t_{PPF}		0.5		5	µs
Start-up Delay Time	t_{STRT}	(Note 13)			100	ms

AC ELECTRICAL CHARACTERISTICS: 1-Wire INTERFACE

(V_{PULLUP} = 2.7V to 5.5V, T_A = -20°C to +70°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
1-Wire INTERFACE REGULAR 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 Time	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
1-Wire INTERFACE OVERDRIVE 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 Time	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

Note 1: $V_{DQ} – V_{THM}$. The THM pin must not be driven to a higher voltage than the DQ pin.

Note 2: The application thermistor cannot exceed the R_{DQ-THM} resistance range over operating temperature. If thermistor mode is not used in the application, it is recommended that a 50KΩ resistor be connected between DQ and THM pins instead.

Note 3: Maximum leakage of DQ pin while in thermistor mode.

Note 4: When performing a Lock Secret (0x6A), Set Overdrive (0x8B) or Clear Overdrive (0x8D) operation, there will be an increased operating current of $I_{PGM-IDLE}$ during and after the program pulse until the next 1-Wire bus reset.

Note 5: See Figure 11 for definitionof t_{PPR}, t_{PPW}, and t_{PPF}.

Note 6: All voltages referenced to VSS.

Note 7: V_{DQ} must be at least 3.0V when the 1-Wire bus is idle.

Note 8: Drive strength at time=0 after Activate Thermistor command is sent to the DS2703.

Note 9: Does not include capacitance referred from VB pin on initial power up.

Note 10: EEPROM data read retention is four years at +50°C

Note 11: Time from msb of Activate Thermistor command until THM pin is driven low internally.

Note 12: Time from msb of Compute Next Secret or Compute MAC command.

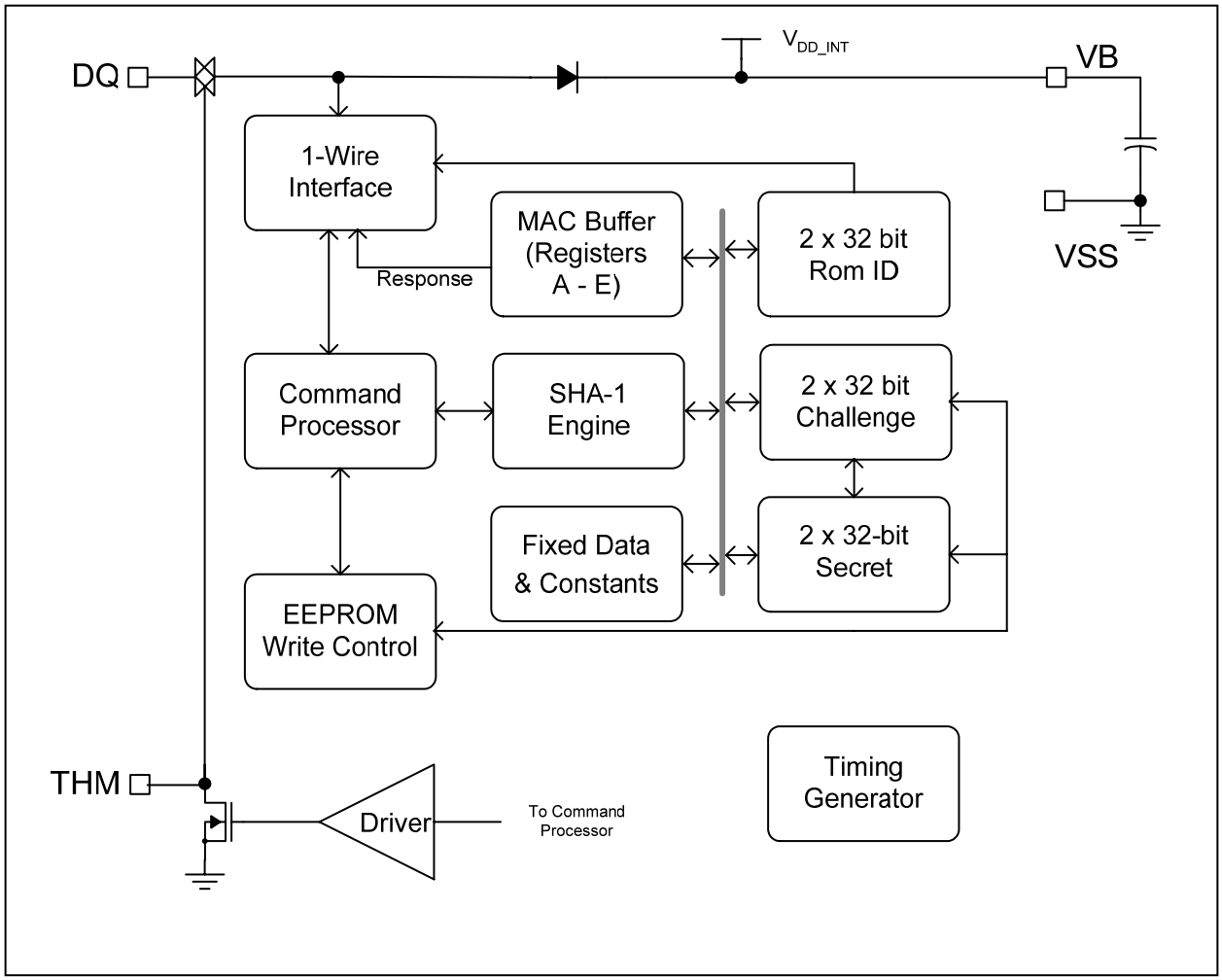
Note 13: Time after initial power up before the DS2703 will respond to communication. T_{STRT} specifications are valid only if the capacitor on VB (C_{VB}) is 0.22µF. Worst case 100ms delay based on maximum thermistor value of 500kΩ.

Note 14: The average current measured in Overdrive mode with minimum bus timings while the master issues: 1-Wire Reset, Skip ROM, Write Challenge, Write 0's repeatedly unil the end of measurement.

PIN DESCRIPTION

8-PIN µMAX	2mm x 3mm TDFN	NAME	FUNCTION
1	7	THM	**Thermistor Mux**. Connect a thermistor from THM to DQ. Optional. For temperature measurements only. If a thermistor is not used in the application, It is recommended THM be tied to DQ with a 50KΩ resistor instead. THM should never be left floating.
2	8	V_{SS}	**Device Ground.** Connect directly to the negative terminal of the battery cell.
3	1	DQ	**Data Input/Output**. 1-Wire data line. Open-drain output driver. Connect this pin to the DATA terminal of the battery pack. This pin has a weak internal pulldown (1µA Typical).
4	2	VB	**Hold-up Supply Bypass Input**. Internal power supply to the DS2703 while DQ is logic low and during thermistor measurement periods. Connect a 0.22µF capacitor from VB to V_{SS}.
5	3	N.C.	**No Connection**. Pin not connected internally, float or connect to V_{SS}.
6	4	N.C.	**No Connection**. Pin not connected internally, float or connect to V_{SS}.
7	5	N.C.	**No Connection**. Pin not connected internally, float or connect to V_{SS}.
8	6	N.C.	**No Connection**. Pin not connected internally, float or connect to V_{SS}.

Figure 1. Block Diagram



DETAILED DESCRIPTION

The DS2703 is comprised of a SHA-1 Authentication function and thermistor mux control that are accessed via a 1-Wire interface. The high voltage (HV) detection circuit routes the externally supplied programming voltage to the EEPROM array and enables the internal regulator to isolate portions of the chip from the programming voltage. The 1-Wire interface controls access by a host system to the 64-bit Net Address (ROM ID) and SHA-1 Authentication.

The DS2703 operates in one of four operating modes: communication, computation, programming and thermistor access. Most operations are performed in communication mode, with the host system addressing the DS2703 using Net Address commands and then setting up an authentication exchange and retrieving the results. In communication mode, the DQ load current is no more than I_{DQ0} maximum, and the DS2703 can be “parasite” powered via the DQ pin through a high impedance pullup resistor during a communication transaction. Power available while the 1-Wire bus is at a logic high is rectified by the on chip diode and stored in an off chip capacitor connected to the VB pin.

In computation mode, when a SHA-1 verification is performed, the DQ load current increases up to I_{DQ2}, necessitating a lower impedance pullup resistor. The computation mode load current occurs after the host supplies the required challenge data and requests the computation using the proper function commands in communication mode. In this mode, the pullup supply and low impedance pullup resistor must be capable of keeping the DQ pin above $V_{PULLUP-MIN}$.

The third operating mode is required when programming the non-volatile memory portions of the DS2703. The programming mode is defined by the application of a high voltage programming pulse to the DQ pin at the appropriate point during a Compute Secret command, Load/Lock Secret or Clear/Set Overdrive Timing command. The internal voltage regulator limits the internal voltage (V_{DD_INT}) to isolate low voltage portions of the chip from the HV programming pulse. Typically, programming mode is used during module or pack manufacture to configure the DS2703 and program the 64-bit secret.

Finally, thermistor mode allows the voltage on an external thermistor to be measured from the DQ line. The command sequence causes the DS2703 to internally disconnect its DQ interface and drive the THM pin to VSS allowing the measurement to be made. The IC remains in this mode until the VB pin capacitor is drained causing the DS2703 to power cycle back to communication mode.

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. An authentication attempt is initiated by the host system providing a 64-bit random challenge then sending one of two compute command sequences. The host and the DS2703 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 DS2703 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. SHA-1 based authentication is a cryptographically strong method in wide use for digitally signing encrypted files and secure transactions such as electronic cash and password exchange protocols.

The FIPS 180 Compliant Input Block, the 512-bit message block is organized as sixteen 32-bit words, W0-W15. The message block is initialized when a command is received to compute the MAC. Upon initialization, the 64-bit secret is loaded, and it is important to note that the SHA-1 algorithm has access to this data, but not the serial interface. The challenge data is received with the command just prior to the compute MAC command. The challenge data is cleared during computation of the MAC, so the host must write new challenge data prior to issuing each Compute MAC or Compute Next Secret command. Additionally, the A, B, C, D and E variables used in the hash computation are initialized per FIPS 180 as shown in Table 1. Variable Initiation. Please contact the factory for memory map details.

Table 1. Variable Initiation

	[31:0]	[23:16]	[15:8]	[7:0]
A	67h	45h	23h	01h
B	EFh	CDh	ABh	89h
C	98h	BAh	DCh	FEh
D	10h	32h	54h	76h
E	C3h	D2h	E1h	F0h

The 160-bit MAC is computed per FIPS 180, including the addition of constants H0-H4. Adding H0-H4 is necessary only to maintain compliance with FIPS 180. The computed MAC is held in the A-E register memory and then returned as a 160-bit serial stream, beginning with the least significant bit of variable A.

Table 2. Message Authentication Code (MAC) Return Format

A[31:24]	**A[23:16]**	**A[15:8]**	**A[7:0]**
B[31:24]	**B[23:16]**	**B[15:8]**	**B[7:0]**
C[31:24]	**C[23:16]**	**C[15:8]**	**C[7:0]**
D[31:24]	**D[23:16]**	**D[15:8]**	**D[7:0]**
E[31:24]	**E[23:16]**	**E[15:8]**	**E[7:0]**

SHA-1 HASH ALGORITHM

General Definitions:

This description of the SHA computation is adapted from the Secure Hash Standard SHA-1 document. The algorithm takes as its input data 16, 32-bit words M_t ($0 \le t \le 15$) as shown in the SHA-1 Input Message Format tables. The SHA computation involves six 32-bit word variables labeled A, B, C, D, E, and TMP, five 32-bit word constants labeled H0, H1, H2, H3, and H4, a sequence of eighty 32-bit words called W_t ($0 \le t \le 79$), a sequence of eighty 32-bit words called K_t ($0 \le t \le 79$), and a Boolean function $f_t(B,C,D)$ ($0 \le t \le 79$). The operations required for the SHA computation are arithmetic addition without carry ("+"), logical inversion or 1's complement ("\"), logical XOR ("⊕"), logical AND ("^"), logical OR ("v"), concatenation of 32-bit values ("|"), assignment (":=") and circular shifting within a 32-bit word. The expression $S^n(X)$ represents a circular shift of X by n positions to the left, with X being a 32-bit word.

The function f_t is defined as follows:

$f_t(B,C,D)$	=	(B^C)v((B\)^D)	($0 \le t \le 19$)
	=	$B \oplus C \oplus D$	($20 \le t \le 39$)
	=	(B^C)v(B^D)v(C^D)	($40 \le t \le 59$)
	=	$B \oplus C \oplus D$	($60 \le t \le 79$)

The sequence K_t ($0 \le t \le 79$) is defined as follows:

K_t	:=	5A827999h	($0 \le t \le 19$)
		6ED9EBA1h	($20 \le t \le 39$)
		8F1BBCDCh	($40 \le t \le 59$)
		CA62C1D6h	($60 \le t \le 79$)

The sequence W_t ($0 \le t \le 79$) is defined as follows:

W_t	:=	M_t (see table, FIPS-180 compliant input block)	($0 \le t \le 15$)
		$S^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16})$	($16 \le t \le 79$)

SHA Computation

The variables A, B, C, D, E and constants H0, H1, H2, H3, and H4 are initialized as follows:

A	:=	67452301h	H0	:=	67452301h
B	:=	EFCDAB89h	H1	:=	EFCDAB89h
C	:=	98BADCFEh	H2	:=	98BADCFEh
D	:=	10325476h	H3	:=	10325476h
E	:=	C3D2E1F0h	H4	:=	C3D2E1F0h

The final values of variables A, B, C, D, and E are generated by looping through the following set of computations for t = 0 to 79 (discarding any carry-out). Finally, the H0-H4 constants are added to the A-E variables respectively, which are then concatenated to form the 160-bit MAC, ABCDE.

for (t = 0 to 79)
{
TMP := $S^5(A) + F_t(B,C,D) + W_t + K_t + E$
E := D
D := C
C := $S^{30}(B)$
B := A
A := TMP
}

160-bit MAC := (A+H0) | (B+H1) | (C+H2) | (D+H3) | (E+H4)

DS2703 AUTHENTICATION COMMANDS

WRITE CHALLENGE [0Ch]. This command writes 64 bits in the message block. The LSB of the 64-bit data 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 Compute MAC and Compute Next Secret (with or without ROM ID) function commands clear the challenge value. Therefore the Write Challenge command **must be issued prior to every** Compute MAC or Compute Next Secret command for reliable results.

***NOTE**: Immediately after power-up, a dummy Compute MAC command is required to initialize the DS2703. 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.*

COMPUTE MAC WITHOUT ROM ID [36h]. This command initiates a SHA-1 computation on the 512 bit block comprised of words W0 - W15. The 64-bit secret and the 64-bit challenge are loaded in the message block and the space in the message reserved for the ROM ID is filled with logical 1's. The DS2703 pauses at least 100us after receiving this command before MAC computation begins. This gives the host ample time to connect the DQ pin to a low impedance node prior to the high current demand computation. The DQ pin must not fall below V_{PULLUP_MIN} during the computation period, t_{COMP}. The host must release the DQ pin for 1-Wire data communications (i.e. terminate the low source impedance mode). After the DQ pin has returned to normal impedance, the host must write eight write zero time slots and then issue 160 read time slots to get the MAC. The 32-bit registers A, B, C, D, and E are used during every cycle of the hash algorithm and their final values at calculation cycle t=79 are added to the values H0-H4 and stored in registers A-E. The new word ABCDE is now the MAC. After issuing the command and waiting a minimum of t_{COMP}, the host reads the 20-byte MAC. This command allows the use of a master secret and message digest response independent of the ROM ID.

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 loaded to the message block. Including the ROM ID unique to each DS2703 in the MAC computation allows the use of a unique secret in each token and a master secret in the host device. See application note “White Paper 4”, available at http://www.maxim-ic.com, for more information.

SHA-1 related commands used while authenticating a battery or peripheral device are summarized in Table 3 for convenience. Four additional commands for clearing, computing and locking of the Secret are described in detail in the following section.

Table 3. Authentication Function Commands

COMMAND	HEX	FUNCTION
Write Challenge	0C	Writes 64-bit challenge for SHA-1 processing. Required prior to either Compute MAC command.
Compute MAC *without* ROM ID and return MAC	36	Computes hash with logical 1's in place of the ROM_ID
Compute MAC *with* ROM ID and return MAC	35	Computes hash including the ROM_ID

SECRET MANAGEMENT FUNCTION COMMANDS

LOAD SECRET [5Ah]. This command changes the 64-bit secret to the provided 64-bit data argument value. The host must apply a programming pulse afterwards to copy the new secret value to EEPROM.

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. The space in the message reserved for the ROM ID is filled with logical 1's. Two words (64 bits) of the output MAC are used as the new secret value. The host must allow t_{COMP} after issuing this command for the SHA calculation to complete, then apply a programming pulse to write the new secret value to EEPROM.

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. Two words (64 bits) of the output MAC are used as the new secret value. The host must allow t_{COMP} after issuing this command for the SHA calculation to complete, then apply a programming pulse to write the new secret value to EEPROM.

***Note**: Please contact the factory for details about what information is used to construct the new secret in the Compute Next Secret With ROM ID and Compute Next Secret Without ROM ID commands.*

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 apply a programming pulse to write the secret lock bit to EEPROM.

Table 4. Secret Loading Function Commands

COMMAND	HEX	FUNCTION
Load Secret	5A	Loads the Secret with 64-bit data argument
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 clears the 1-Wire Overdrive bit to select the Standard 1-Wire timings shown in the Electrical Characteristics table. The Overdrive bit is stored in EEPROM so that the programmed speed selection can be recalled on initial power up. The host must apply a programming pulse to complete the command.

SET OVERDRIVE [8Bh]. This command sets the 1-Wire Overdrive bit to select the Overdrive 1-Wire timings shown in the Electrical Characteristics table. The Overdrive bit is stored in EEPROM so that the programmed speed selection can be recalled on initial power up. The host must apply a programming pulse to complete the command.

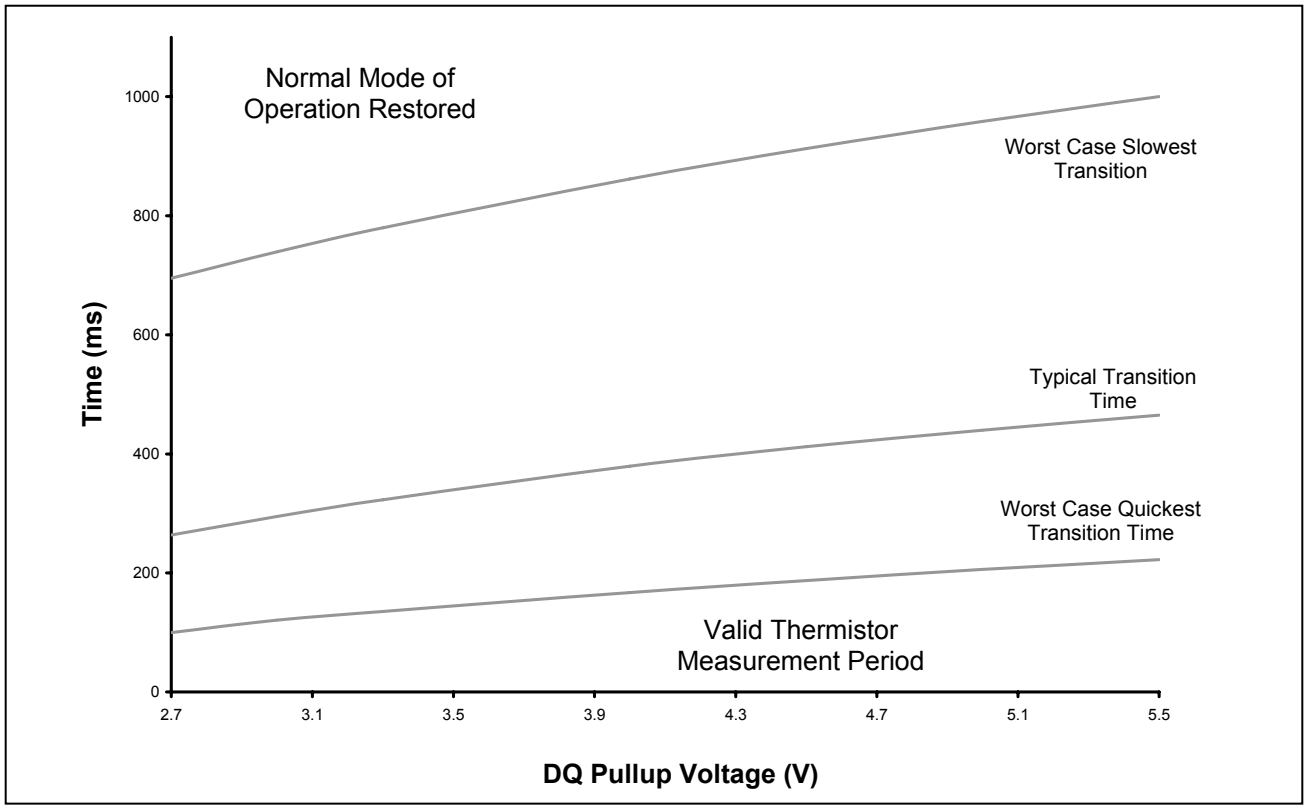
Table 5. 1-Wire Speed Control Function Commands

COMMAND	HEX	FUNCTION
Clear Overdrive	8D	Clears the Overdrive 1-Wire Speed bit to select Standard 1-Wire timings
Set Overdrive	8B	Sets the Overdrive 1-Wire Speed bit to select Overdrive 1-Wire timings

THERMISTOR MEASUREMENT

The DS2703's 1-Wire interface allows a thermistor to be multiplexed on the DQ line for thermal measurements of the cell pack without adding an additional pack connection. See the Typical Operating Circuit, Figure 5. The thermistor is connected between the DQ and THM pins. THM is normally high impedance to prevent the thermistor from interfering with 1-Wire communication. When an Activate THM command is received, THM is internally driven to VSS and the DQ pin becomes high impedance allowing the thermistor resistance to be measured. See the timing diagram in Figure 12.

Figure 2. Thermistor Mode Duration when C_{VB} is .22µF



The DS2703 will remain in thermistor measurement mode until the stored charge on the VB pin capacitor is depleted causing the IC to power cycle back to standard mode of operation. While in thermistor measurement mode, communication to the DS2703 is not possible. After measuring the thermistor, the host must wait until the VB capacitor is depleted. Figure 2 shows the typical and worst case transition times over the full operating range when using .22µF as the VB pin capacitor. Thermistor measurements should be made within the first 100ms after issuing the command. The host system should then wait until at least 1000ms have passed before sending the next communication sequence to the IC.

Table 6. Thermistor Function Command

COMMAND	HEX	FUNCTION
Activate Thermistor	A9	Activates the THM output for thermistor measurement. Activation occurs within 50µs of command completion and continues until VB capacitor depleted.

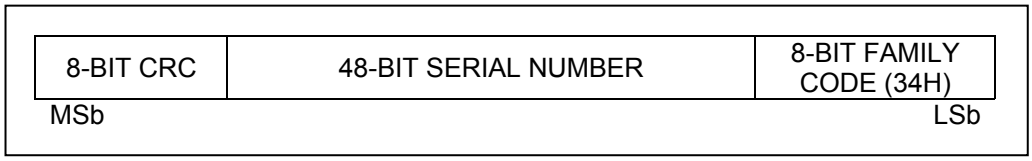
1-Wire BUS SYSTEM

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 DS2703 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 DS2703 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 earlier Dallas 1-Wire product documentation. The first eight bits of the Net Address are the 1-Wire family code, (34h) for the DS2703. 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 3.). The 64-bit net address and the 1-Wire I/O circuitry built into the device enable the DS2703 to communicate through the 1-Wire protocol detailed in this data sheet.

Figure 3. 1-Wire Net Address Format



CRC GENERATION

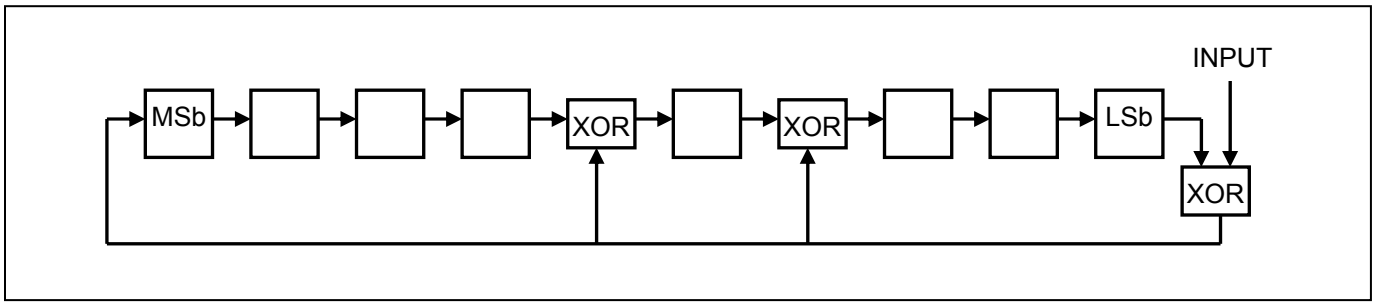
The DS2703 has an 8-bit CRC stored in the most significant byte of its 1-Wire net address. To ensure error-free transmission of the address, the host system can compute a CRC value from the first 56 bits of the address and compare it to the 8-bit CRC from the DS2703.

The host system is responsible for verifying the CRC value and taking action as a result. The DS2703 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 4, 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 Touch Memory Products* (www.maxim-ic.com/appnoteindex).

In Figure 4, 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 4. 1-Wire CRC Generation Block Diagram

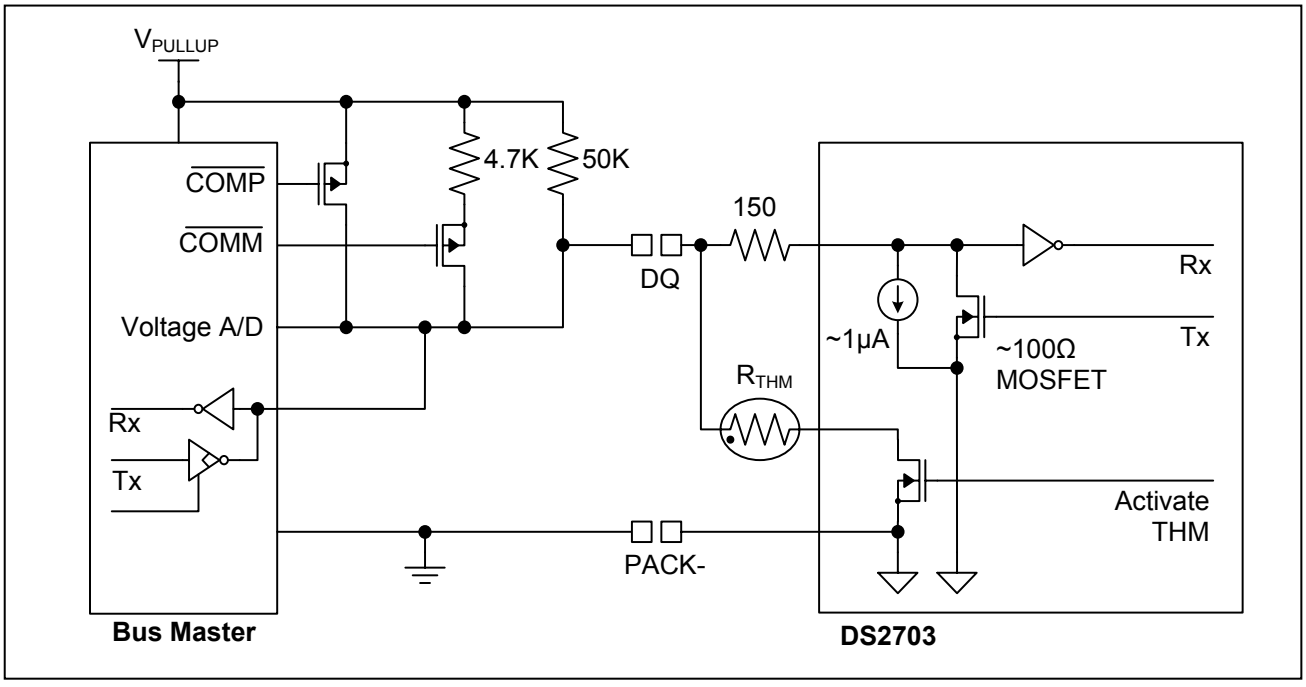


HARDWARE CONFIGURATION

The DS2703 uses an open-drain output driver as part of the bidirectional interface circuitry shown in Figure 5. If a bidirectional pin is not available on the bus master, separate output and input pins can be connected together. For normal communication the 1-Wire bus must have a pullup resistor at the bus-master end of the bus. For short line lengths and/or V_{PULLUP} ≥ 3.0V, a value of approximately 4.7kΩ is recommended. For long line lengths and/or V_{PULLUP} < 3.0V, a value of approximately 2kΩ 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_{LOW0}, slave devices on the bus begin to interpret the low period as a reset pulse, effectively terminating the transaction.

When performing SHA-1 computations with a low pullup voltage, the DS2703 may require a stronger pullup than 4.7k to maintain the minimum V_{PULLUP} requirement. A P-FET in parallel with the standard pullup can be switched on during computation and then disabled to read the result. When measuring the thermistor R_{THM}, both the strong pullup and standard pullup should be disabled to allow a weak pullup to form a voltage divider with the thermistor. A voltage A/D connected directly to the 1-Wire bus can then read the voltage drop of the thermistor.

Figure 5. 1-Wire Bus Interface Circuitry



TRANSACTION SEQUENCE

The protocol for accessing the DS2703 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 DS2703 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 *1-Wire 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. Figure 6 presents a transaction flowchart of the net address commands.

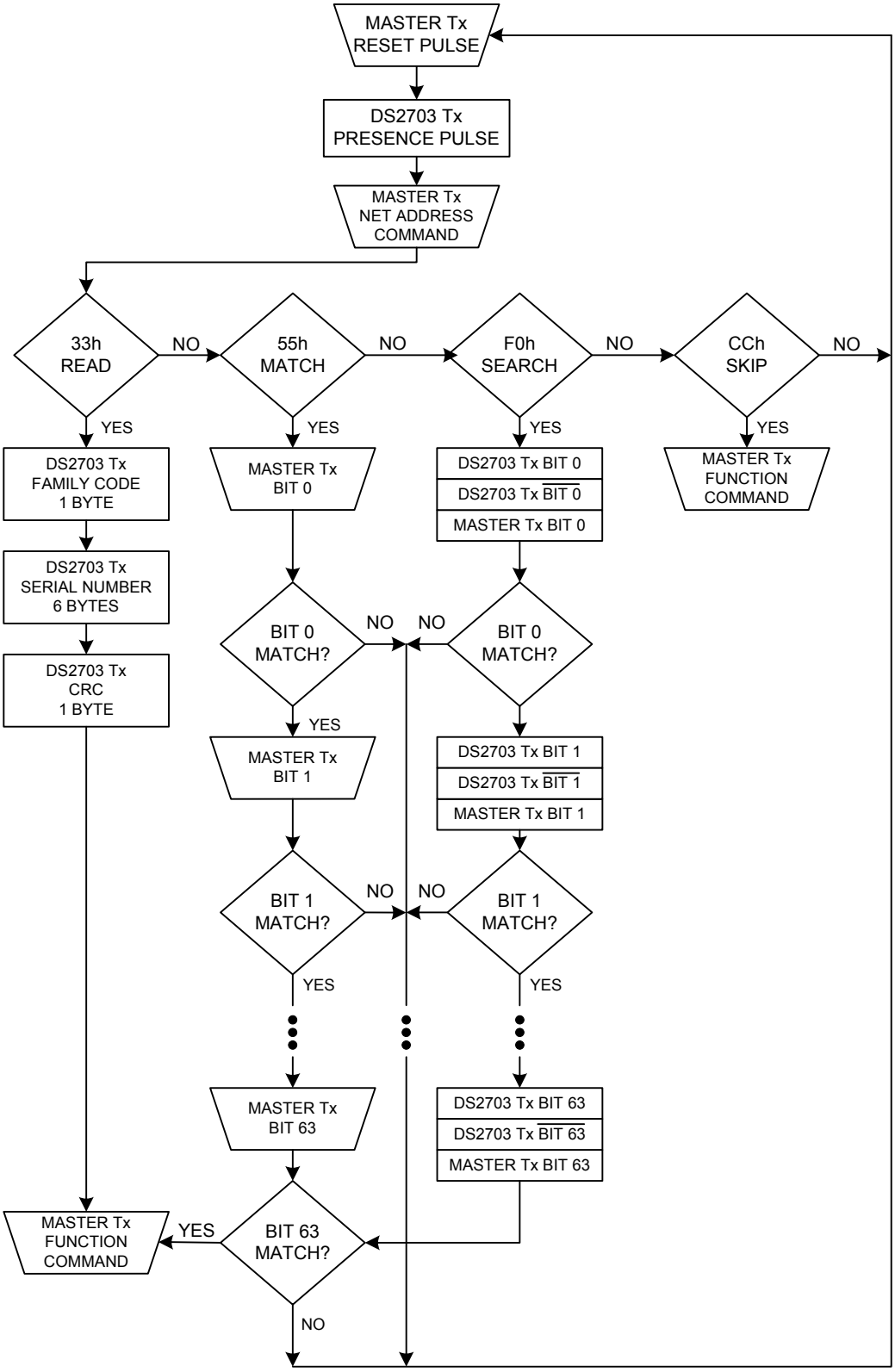
Read Net Address [33h]. This command allows the bus master to read the DS2703's 1-Wire net address. This command can only be used if there is a single slave on the bus. If more than one slave is present, a data collision occurs when all slaves try to transmit at the same time (open drain produces a wired-AND result).

Match Net Address [55h]. This command allows the bus master to specifically address one DS2703 on the 1-Wire bus. Only the addressed DS2703 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 DS2703 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 DS19xx iButton® Standards* for a comprehensive discussion of a net address search, including an actual example (www.maxim-ic.com/iButtonBook).

Figure 6. Net Address Command Flow Chart

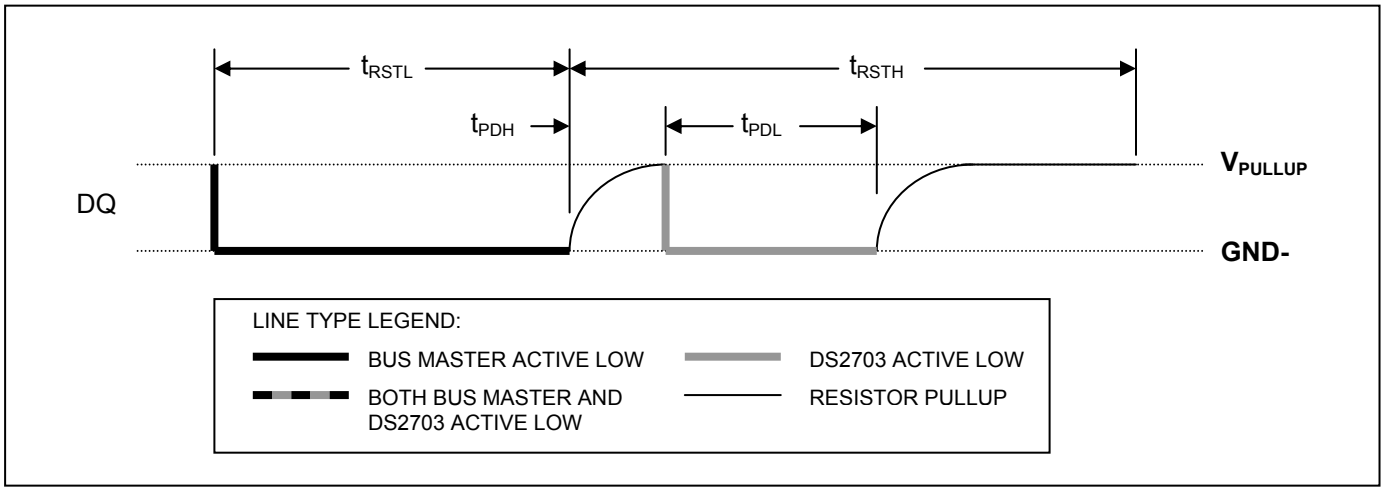


I/O SIGNALING

The 1-Wire bus requires strict signaling protocols to ensure data integrity. The four protocols used by the DS2703 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 DS2703 is shown in Figure 7. A presence pulse following a reset pulse indicates that the DS2703 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 DS2703 waits for t_{PDH} and then transmits the presence pulse for t_{PDL}.

Figure 7. 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 DS2703 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 8. 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.

***Caution**: When communicating in standard mode, the number of consecutive Write 0 time slots with t_{LOW0} = t_{LOW0_MAX} and t_{REC} = t_{REC_MIN} is limited to 64. If more than 64 Write 0 time slots with t_{LOW0} = t_{LOW0_MAX} and t_{REC} = t_{REC_MIN} are issued, the internal supply (V_{DD_INT}) can drop so low that the DS2703 resets. Increasing t_{REC} to 5µs allows Vdd_int to recharge sufficiently each 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 DS2703 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 DS2703 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 8 and the timing specifications in the Electrical Characteristics table for more information.

Figure 8. 1-Wire Write and Read Time Slots

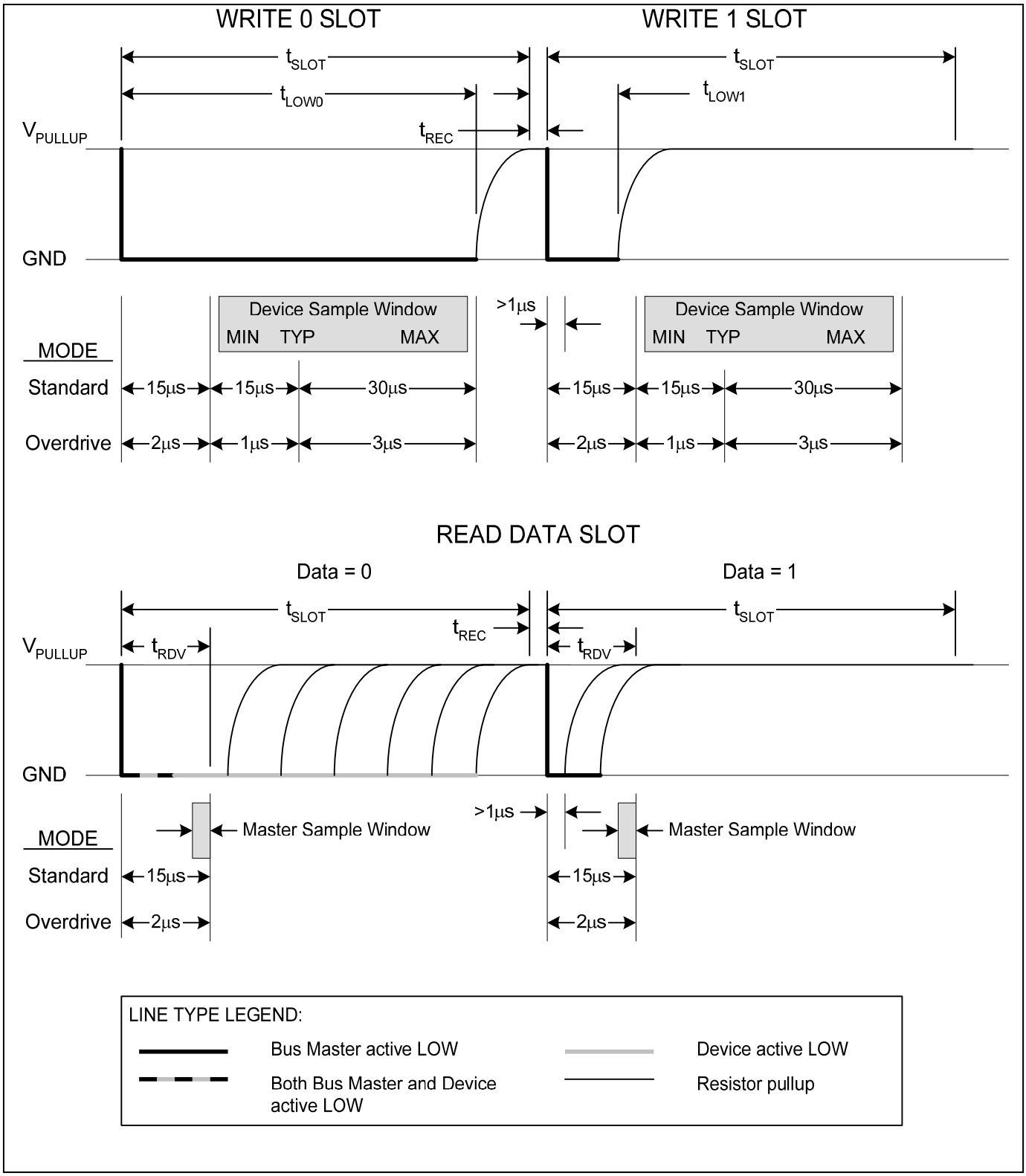


Table 7. All Function Commands

COMMAND	HEX	FUNCTION
Write Challenge	0C	Writes 64-bit challenge for SHA-1 processing. Required prior to all Compute MAC and Compute Next Secret commands.
Compute MAC *without* ROM_ID and return MAC	36	Computes hash of W0-W15 with logical 1's in place of the ROM_ID.
Compute MAC *with* ROM_ID and return MAC	35	Computes hash of W0-W15 with the ROM_ID.
Load Secret	5A	Writes the 64-bit Secret to supplied data. Requires programming voltage on DQ.
Compute Next Secret *without* ROM ID	30	Generates new global secret. Requires programming pulse.
Compute Next Secret *with* ROM ID	33	Generates new unique secret. Requires programming pulse.
Lock Secret	6A	Sets lock bit to prevent changes to the Secret. Requires programming pulse.
Set Overdrive	8B	Sets 1-Wire interface timings to OVERDRIVE. Requires programming pulse.
Clear Overdrive	8D	Sets 1-Wire interface timings to STANDARD. Requires programming pulse.
Activate Thermistor	A9	Activates the THM output for thermistor measurement. Activation occurs within 50µs of command completion and continues until the VB capacitor is discharged.
Reset	BB	Resets DS2703 (Software POR).

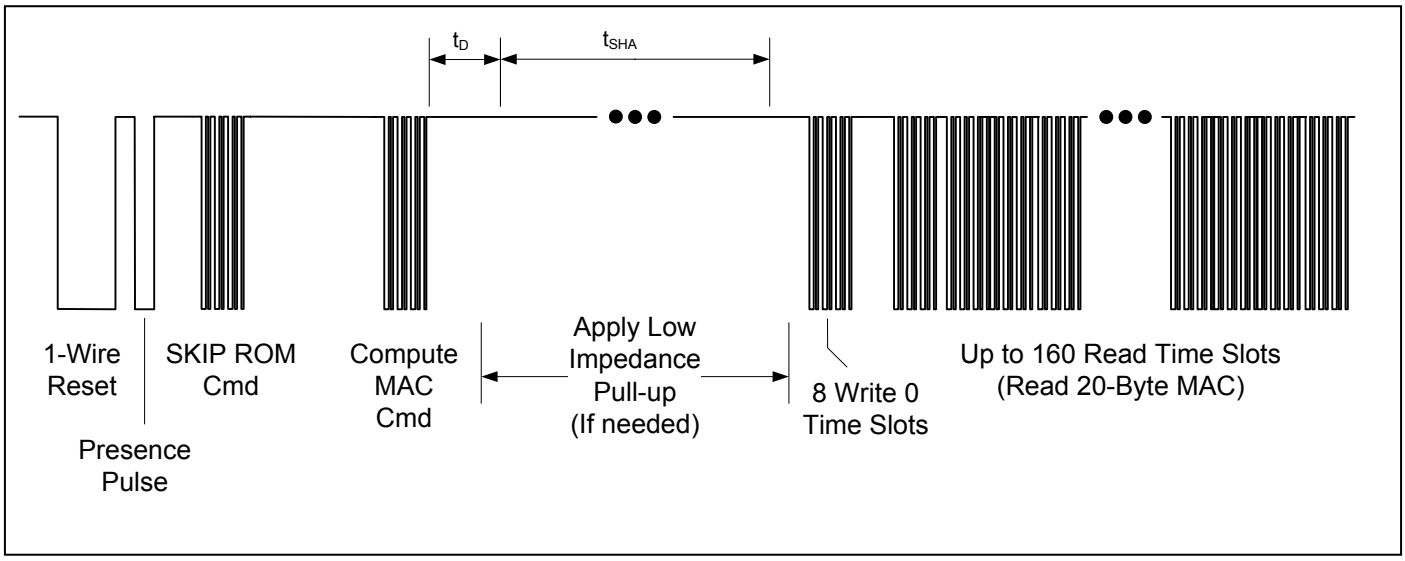
Table 8. Guide to Function Command Requirements

COMMAND	STRONG PULLUP ON DQ	ISSUE 00h BEFORE READ	READ/WRITE TIME SLOTS	PROGRAMMING PULSE
Write Challenge			Write: 64	
Compute MAC	**X**	**X**	Read: up to 160	
Compute Next Secret	**X**			**X**
Lock Secret, Set/Clear Overdrive				**X**
Load Secret			Write: 64	**X**
Reset				

LOW-IMPEDANCE DQ DURING COMPUTATION

The SHA-1 computation requires more current than the DQ pullup resistor used during normal communication can supply. During the computation, the DQ source impedance must be reduced to maintain power to the device under the higher load condition. The user must connect the low impedance source to the DQ line within t_D of issuing any command to perform a computation, and return the DQ source to normal settings before reading or writing to the one-wire interface. See Figure 9.

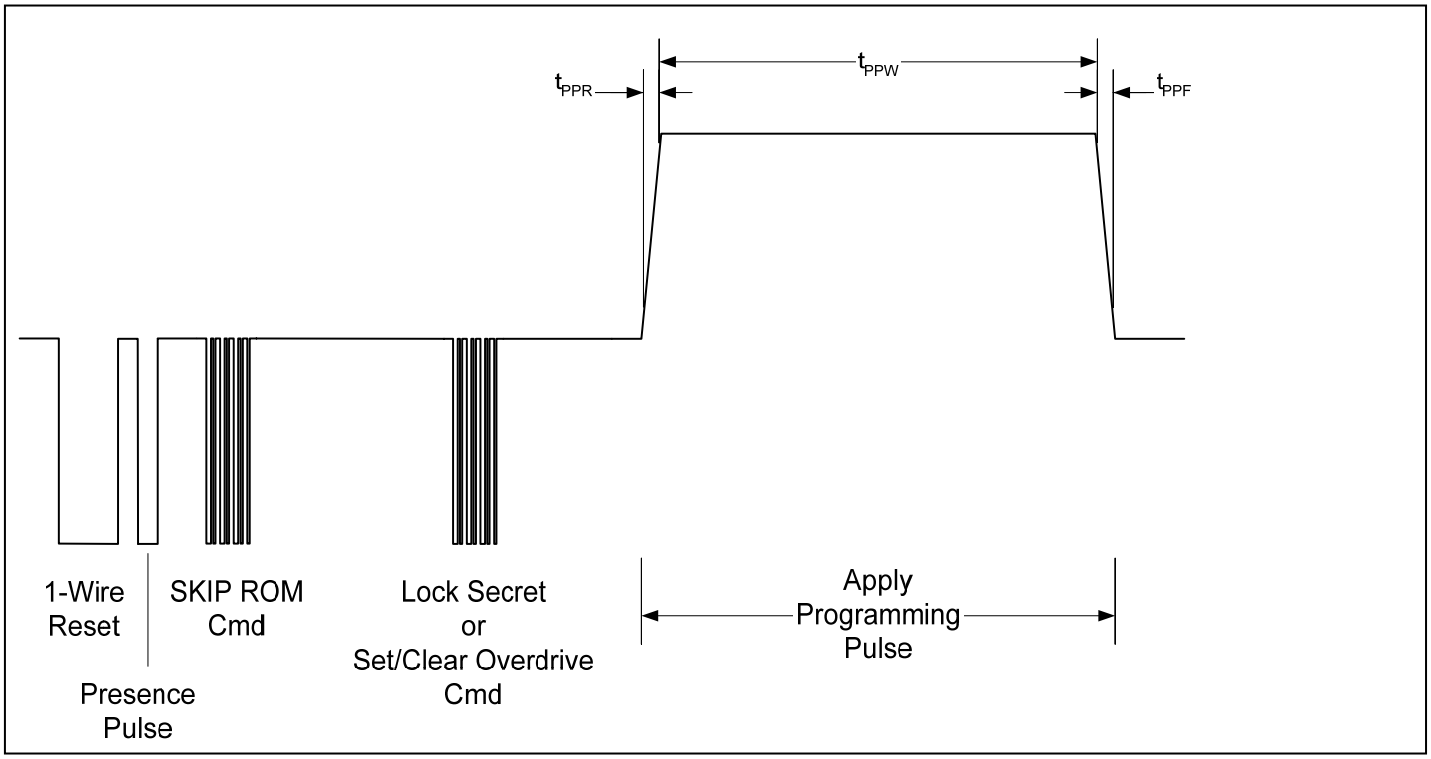
Figure 9. Compute MAC Function Command



PROGRAMMING PULSE

A typical programming waveform is shown in Figure 10. The user issues a 1-Wire reset followed by a Skip ROMID command, Match ROMID plus the ROMID, Search or Read Net, the Load Secret command and then the two 32-bit words to be loaded into EEPROM. The DQ line is then pulled to V_{PP} for t_{PPW} milliseconds and then returned to nominal voltage. The fast rise and fall time requirements for the programming pulse are required to prevent damage during the transition between normal communication mode and programming mode.

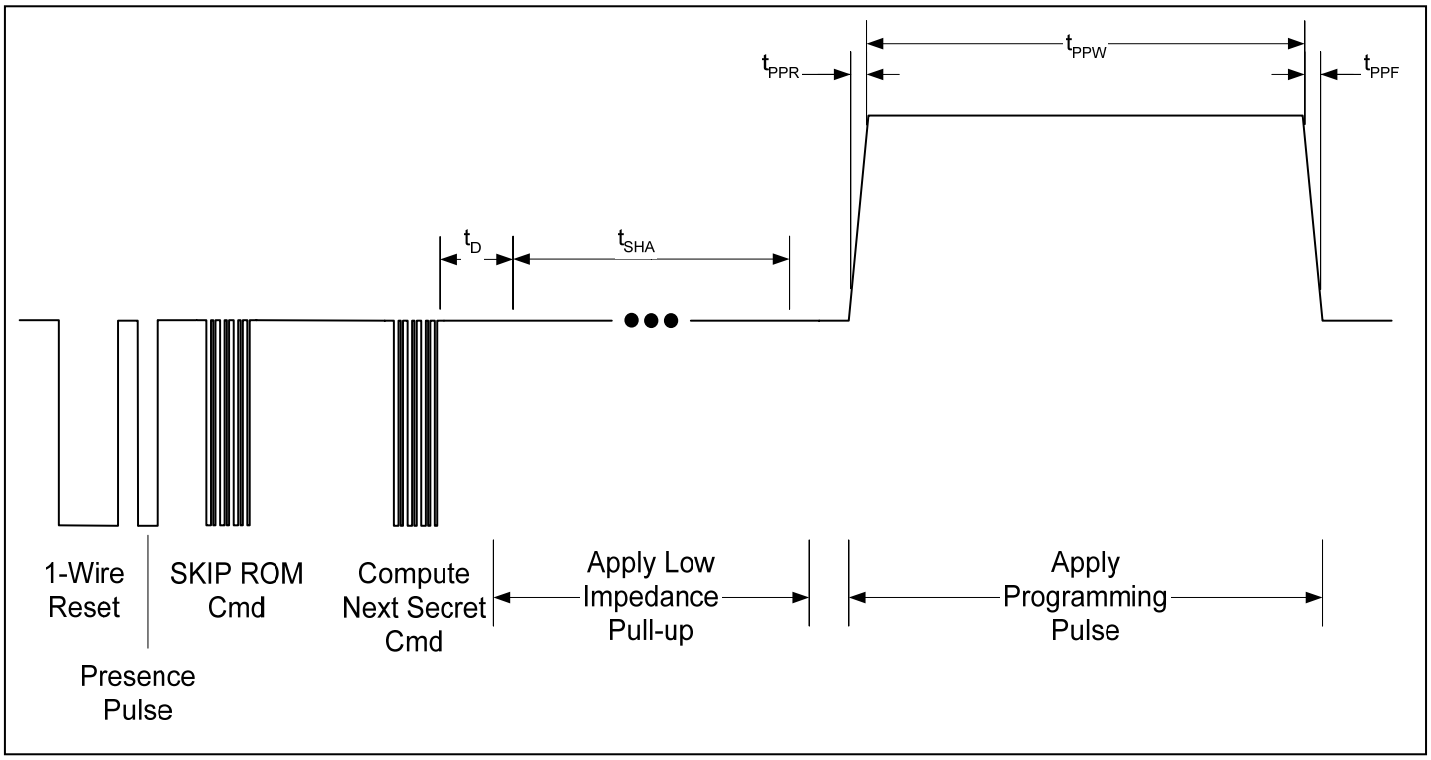
Figure 10. Lock Secret, Set/Clear Overdrive Function Commands



COMPUTATION AND PROGRAMMING

The Compute Next Secret operation waveform is shown in Figure 11. The user issues a 1-Wire reset followed by a Skip ROMID command, Match ROMID plus the ROMID, Search or Read Net, followed by the Compute Next Secret command. The system host must connect the low impedance source to the DQ line within time t_D and for a duration of time t_{SHA}. The DQ line is then pulled to V_{PP} for t_{PPW} milliseconds and then returned to nominal voltage. The fast rise and fall time requirements for the programming pulse are required to prevent damage during the transition between normal communication mode and programming mode.

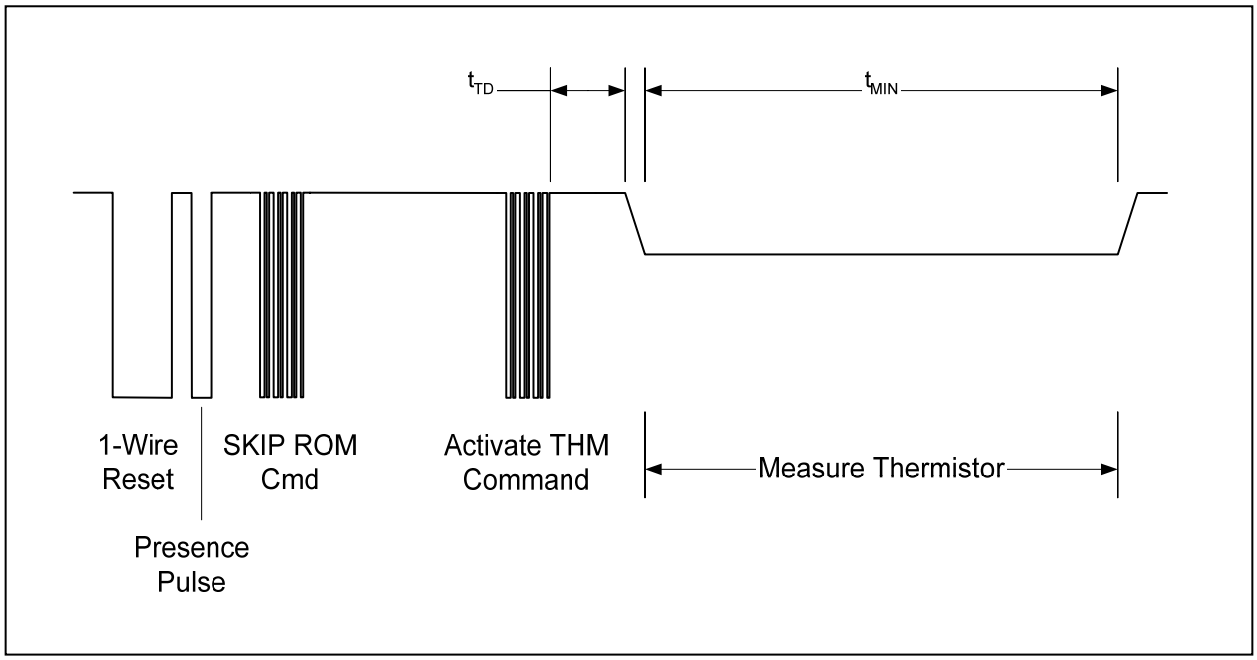
Figure 11. Compute Next Secret Function Command



HIGH-IMPEDANCE DQ FOR THERMISTOR MEASUREMENT

The user issues a 1-Wire reset followed by a Skip ROMID command, Match ROMID plus the ROMID, Search or Read Net, followed by the Activate Thermistor command. Within the time period t_{TD} the DS2703 disables its DQ input and internally drives the THM pin low. Immediately following the Activate Thermistor command, the host system should enable the weak pullup to VCC and then measure the thermistor by sampling the voltage level of the 1-Wire bus within time t_{MIN}. The DS2703 automatically reverts back to communication mode after t_{MIN}. See Figure 12.

Figure 12. Activate Thermistor Command



PACKAGE INFORMATION

(The package drawing(s) in this data sheet may not reflect the most current specifications. For the latest package outline information, go to **www.maxim-ic.com/DallasPackInfo**.)