PRELIMINARY

DS1954 TECHNICAL INFORMATION
Cryptographic iButton™

SECURITY FEATURES

- Single–chip, physically secure coprocessor for unsecure host
- Arithmetic accelerator executes 1024–bit public key cryptography in less than 1 second
- Unresettable True Time Clock self–imposes expiration dates
- Durable stainless steel case clearly shows visual evidence of physical tampering
- 6K bytes NVSRAM zeroes itself in response to tampering or cooling below –30°C
- 32K bytes of ROM stores unalterable validated firmware as Software ICs
- Unique, factory–lasered 64–bit registration number (8–bit family code + 48–bit serial number + 8–bit CRC tester) assures absolute traceability because no two parts are alike
- Multi–drop controller supports multiple iButtons on the same signal line for n–factor security
- Signal path to the chip is limited to the lid of the iButton to enhance security
- Communication protocol includes 16–bit CRCs to insure error free packet transfers to the buffer memory even with intermittent connection
- The iButton can be accessed while affixed to a wearable accessory to lower the chance of being lost or stolen
- Only an authorized service provider can install a transaction file which programs the iButton for a specific application
- The transaction file contains scripts that call on tested pre–fabricated cryptographic functions
- Each file can be locked after installation so that additional transaction files for new services may be installed without interference

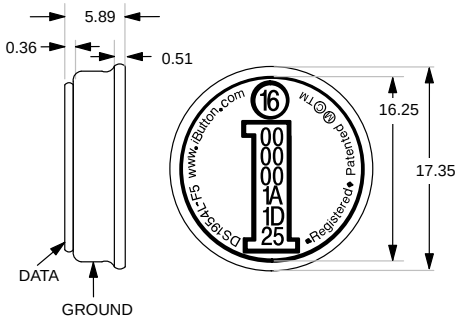
GENERAL FEATURES

- Overdrive mode boosts communication speed from 16.3k to 142k bits per second
- Operating temperature range from –20°C to +70°C
- Over 10 years of data retention
- Timing accuracy better than ± 2 minutes/month at 25°C
- Button shape is insensitive to angular orientation and self–aligning with the Dot receptor
- The iButton is easily affixed with self–stick adhesive backing, latched by its flange, or locked with a ring pressed onto its rim
- Mechanical specification and 1–Wire™ communication follow the iButton Book Of Standards
- Meets UL#913 (4th Edit.); Intrinsically Safe Apparatus, Approved under Entity Concept for use in Class I, Division 1, Group A, B, C and D Locations (application pending)

SUPPORT

- Script tool kit speeds the development of applications such as micro cash meters or stored value purses
- Adapters for LPT port (parallel), COM Port (serial), ETHERNET (10–base–T), or SCSI connectivity

F5 MICROCAN™



All dimensions are shown in millimeters.

ISSUING AND ACTIVATION INFORMATION

See www.ibutton.com

EXAMPLES OF ACCESSORIES

DS1410E	Parallel Port Button Holder
DS1402D–DB8	iButton Dot Receptor
DS9093F	Snap–In Fob
DS9096P	Self–Stick Adhesive Pad
DS9093RA	Mounting Lock Ring
DS9101	Multi–Purpose Clip

CRYPTO iBUTTON DESCRIPTION

The DS1954 Crypto iButton is a secure coprocessor residing in a stainless steel MicroCan with 1–Wire interface. The device is addressed by matching its individual 64–bit factory–lasered registration number. The 64–bit number consists of an 8–bit family code, a unique 48–bit serial number, and an 8–bit cyclic redundancy check. Data is transferred serially via the 1–Wire communication protocol which requires only a single data lead and a ground return for communication and power. Typical applications include authentication of the person at the computer, secure transmission of E–mail, electronic notary service, electronic cash dispenser, electronic secure monetary transactions, software authorization and usage metering, postal metering service, electronic signature, micro–cash metering and physically secure coprocessor array for servers.

OVERVIEW

The block diagram in Figure 1 shows the relationships between the major control and memory sections of the DS1954. The DS1954 has four main components: 1) 64–bit lasered ROM, 2) I/O and status registers, 3) microcomputer with 32K byte firmware and 6K byte nonvolatile data memory, and 4) arithmetic accelerator for modular arithmetic. The device derives its power for I/O communication entirely from the 1–Wire communication line by storing energy on an internal capacitor during periods of time when the signal line is high and continues to operate off of this “parasite” power source during the low times of the 1–Wire line until it returns high to replenish the parasite (capacitor) supply. During program execution, the 1–Wire line must be pulled high to 5V via a low–impedance transistor to provide the energy for the microcomputer and the accelerator to operate. After a time period that was agreed between bus master and Crypto iButton, the DS1954 stops executing the program and waits for the bus master to initiate another processing cycle and so on, until data processing is finished. The timing is based on the True Time Clock of the DS1954 and the Real Time Clock of the bus master.

The hierarchical structure of the 1–Wire protocol is shown in Figure 2. The bus master must first provide one of the six ROM Function Commands, 1) Read ROM, 2) Match ROM, 3) Search ROM, 4) Skip ROM, 5) Overdrive–Skip ROM or 6) Overdrive–Match ROM. Upon completion of an Overdrive ROM command byte executed at regular speed, the device will enter the Overdrive mode where all subsequent communication occurs at a higher speed. These commands operate on the 64–bit lasered ROM portion of each device and can singulate a specific device if many are present on the 1–Wire line as well as indicate to the bus master how many and what types of devices are present. After a ROM function command is successfully executed, the data transfer and control functions that operate the microcomputer inside the DS1954 become accessible and the bus master may issue any one of the nine commands specific to the DS1954.

64–BIT LASERED ROM

Each DS1954 contains a unique ROM code that is 64 bits long. The first eight bits are a 1–Wire family code. The next 48 bits are a unique serial number. The last eight bits are a CRC of the first 56 bits. (See Figure 3). The 64–bit ROM and ROM Function Control section allow the DS1954 to operate as a 1–Wire device and follow the 1–Wire protocol. The functions required to operate the microcomputer and accelerator of the DS1954 are not accessible until the ROM function protocol has been satisfied.

The 1–Wire CRC of the lasered ROM is generated using the polynomial $X^8 + X^5 + X^4 + 1$. Additional information about the Dallas Semiconductor 1–Wire Cyclic Redundancy Check is available in the “Book of DS19xx iButton Standards.” The shift register acting as the CRC accumulator is initialized to zero. Then starting with the least significant bit of the family code, one bit at a time is shifted in. After the eighth 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. Shifting in the eight bits of CRC should return the shift register to all zeroes.

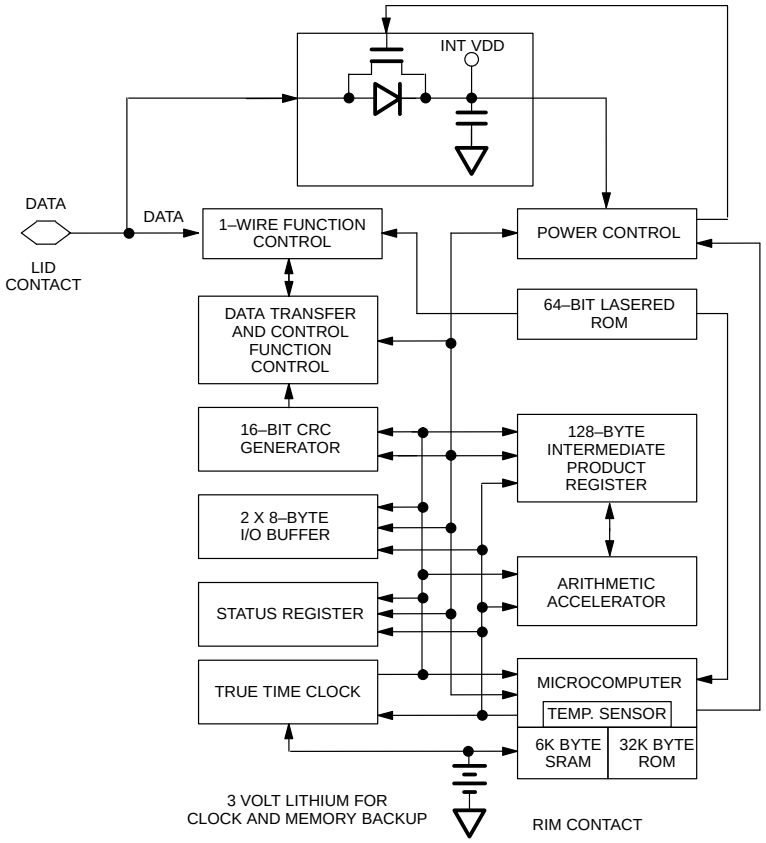
DATA AND CONTROL REGISTERS

From the application software developers perspective, the DS1954 looks like two registers and a buffer and control logic that are accessed through a 1–Wire bus (Figure 1). After the Intermediate Product Register (IPR) and the I/O buffer have been loaded with data and control information, the microcomputer will be started, perform the requested tasks and place the result into the IPR from where it can be read by the bus master. The data processing inside the DS1954 and the structure of the data packets that tell the microcomputer what tasks to perform is governed by the ROM firmware. A detailed description of the firmware functions and data packet formats is found in the "Crypto iButton Firmware Reference Manual."

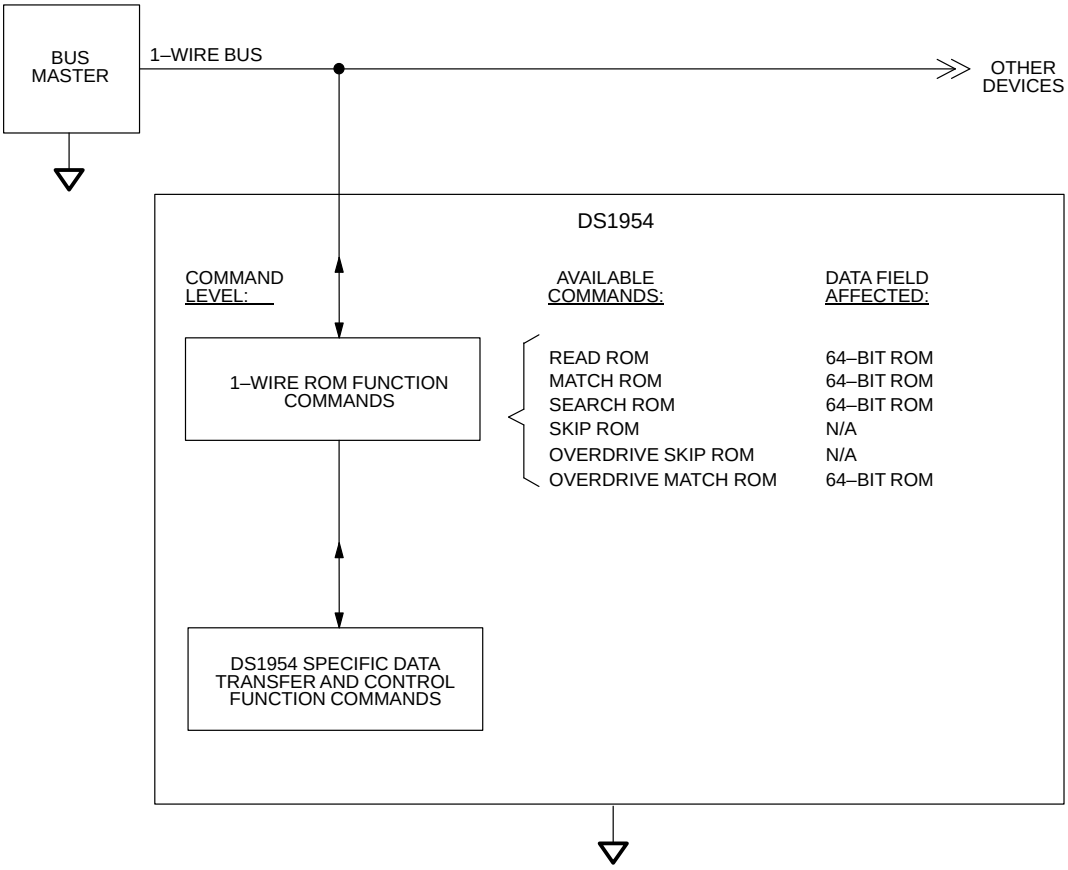
The IPR is normally used to transfer command codes and message data to the microcomputer in blocks of up to 128 bytes and to receive results back from the microcomputer. The messages themselves may extend over several blocks. The message transfer management, which includes block number, block length, bytes remaining, CRC and checksum, is controlled by means of the I/O buffer. During extensive mathematical operations, the microcomputer will pause after a predefined amount of time and allow the bus master to read progress information from the status register. The bus master will then signal the microcomputer to resume computation until the next pause occurs, and so on, until the task is finished.

The duration of the computation time slices is controlled by the True Time Clock. Other functions of the True Time Clock are date/time stamping of events and imposing expiration dates. The arithmetic accelerator is optimized for exponentiation, multiplication and squaring. Such operations are typically required for de–/encryption of data packets that use the large number theory of public key cryptography.

DS1954 FUNCTIONAL BLOCK DIAGRAM Figure 1



HIERARCHICAL STRUCTURE FOR 1–WIRE PROTOCOL Figure 2



64–BIT LASERED ROM Figure 3