

FRIEND



OR FOE: Battery-authentication ICs separate the good guys from the bad

ALL BATTERY PACKS ARE NOT CREATED EQUAL: UNAUTHORIZED AFTER-MARKET PACKS MAY CONTAIN CELLS THAT CAN SELF-DESTRUCT WHEN YOU CHARGE THEM AT THE HIGHER VOLTAGES THAT NEW LITHIUM-ION TECHNOLOGIES DEMAND. BATTERY-AUTHENTICATION ICs USE ADVANCED SECURITY METHODS TO WEED OUT COUNTERFEITS.

Battery packs for consumer applications, such as cell phones and laptops, continue to move further away from the one-size-fits-all category. The responsibility for ensuring that only compatible packs plug into recharging systems again belongs to the system designer to authenticate a battery pack before charging it. To decide which authentication scheme is right for your design, you need to weigh the cost, size, and security level that chip vendors' authentication approaches are now offering.

Battery-pack authentication is necessary because the lithium-ion cells that are the building blocks of all such packs are changing, and, although they still may have the same physical dimension, their input charging voltage and required charging rates are changing and fragmenting across markets (Reference 1). If the cells charge at the wrong voltage or too quickly, they may explode. Vendors can ship their products with the proper battery pack, only to find that customers go the after-market route to replace or back up battery packs because after-market packs are easy to find and usually cheaper. Counterfeit battery packs pose a threat to user safety (Reference 2).

In 2004, cell-phone manufacturers Kyocera and LG both had to recall branded, counterfeit battery packs that lacked the necessary overcharging circuits to prevent overheating and explosions. To combat such problems, one cell-phone manufacturer, Nokia, places holograms on its approved battery packs. Customers can check the code on the hologram online to verify whether a part is genuine. However, this approach assumes that the customer shares the manufacturer's concern about the battery pack's quality and authenticity and can evaluate the authenticity of the hologram label. A more active approach to verifying packs is to build authentication into the charging system (see sidebar "A primer on security cracking").

The lowest level of authentication is to verify that the battery works basically as a user expects. To perform such authentication, place a resistor into the pack and measure the voltage drop. The next level relies on reading a code in the pack that contains parameters such as battery ID, manufacturing date, and cell voltage. These parameters are easy to read and duplicate, however. The highest level of security uses a challenge-response procedure between the system host and a cryptographic-authentication IC in the battery pack (Figure 1). The host system can be an external, separate battery-pack charger, but, for cell phones and laptops, the battery pack usually charges while it's in the device rather than in an external charger. The authentication IC within the battery pack answers the host query

AT A GLANCE

After-market battery packs may be unable to handle the higher charging voltages that new lithium-ion technologies require, potentially leading to unsafe, explosive conditions.

Host systems need to authenticate battery packs before recharging.

Authentication ICs handle the complexity of using security algorithms to validate packs.

with a response that its security algorithm and a secret key code in the device determine.

Authentication ICs' security level depends on the complexity of their encoding algorithms. The three popular techniques that authentication ICs use are CRC (cyclic redundancy check), SHA-1 (Secure Hash Algorithm-1), and proprietary vendor algorithms (Table 1).

HASHING OR ENCRYPTION

Hashing algorithms calculate a signature for the system inputs and are not, strictly speaking, encryption algorithms, although people commonly refer to them as such. Encryption algorithms are two-way, allowing unlimited encoding and decoding of data streams. Hashing functions are one-way: You can't regain the input data from the signature. The NIST (National Institute of Standards

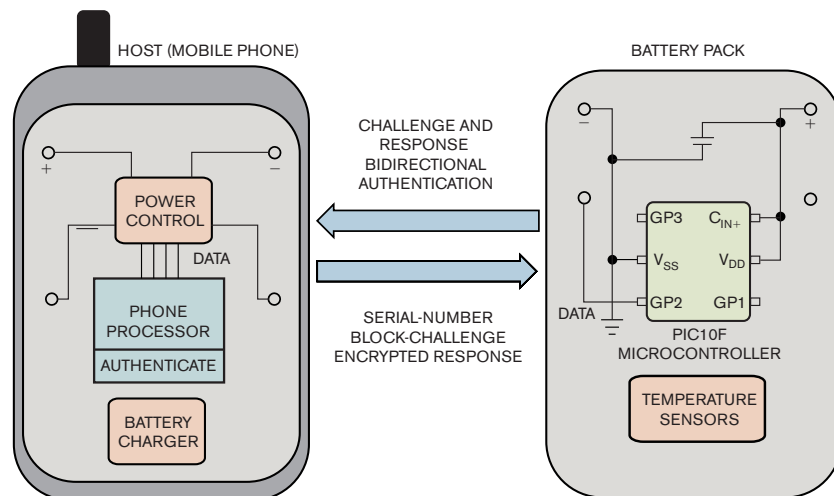


Figure 1 The host system issues a challenge to the battery pack and waits for the proper response before beginning charging to ensure that the pack is authentic (courtesy Microchip).

and Technology) created the SHA-1 (pronounced "Shaw-one") hashing algorithm, the most popular security algorithm. It powers the NIST's digital-signature standard (references 3 and 4).

New ICs are offering this algorithm, measuring how seriously companies are taking battery authentication. Previously, they would have considered this feature as overkill for this application. For example, Maxim has introduced the DS2704, a SHA-1 based device, as an upgrade from the DS2502, which provides ID information only with no

encryption. The DS2704 is backward-compatible with the 2502 instruction set and has an additional page of EEPROM for storing battery-condition information, such as amount of charge.

SHA-1's high security level comes at a cost: The die for such a chip must be larger because of the more complex algorithm. Jon Qian, senior member of the technical staff at Texas Instruments, which makes the CRC-based bq26150 IC, defends the CRC as a cost-effective security measure: "SHA-1 is well-known; banks use it for financial transactions, but this level of complexity requires a bigger die and more internal memory. CRC-based authentication is still difficult to break but still gives a decent die-size implementation." He concedes that high-security requirements warrant SHA-1. For example, TI plans to introduce the SHA-1-based bq26100 chip in the second quarter.

Arman Naghavi, vice president of Intersil's Handheld Power group, says that determining the amount of security you need requires balancing the life of a consumer product and the cost of the security feature. You can think of the robustness of a security algorithm in the years of computer processing it takes to break it. Intersil's ISL9206 uses the company's proprietary Flexihash+ security algorithm; Naghavi claims that it would take three Pentium 4 processors 10 years to break the code. Consumer products

A PRIMER ON SECURITY CRACKING

Gene Armstrong, managing director of thermal and battery management for Maxim, lists several ways to attack a security system for a battery pack: "One attack method is to use brute-force computing: You issue a challenge, review the response, and emulate that function on a very fast computer, looking for the secret key that generated that challenge-response pair.

The problem with brute force is that it takes 280 years to find a 64-bit secret. A 3-GHz processor can execute a SHA-1 test in about 220 nsec. To check all combinations would require 3.9^{12} sec, or about 125,000 years. Even when 10,000 engines are

running in parallel at 3 GHz, this method doesn't guarantee a match for 12.5 years."

A second technique, side-channel attack, looks for a manufacturing-test mode to exploit. Armstrong points out that Maxim's DS2704 has no test modes that read the secret: For test, Maxim looks at an AND of all the bits and an OR, to ensure that that portion of the IC is working.

A third type of attack would be a physical one. Maxim bases its parts on a three-metal process, with a final metallized-silicon layer, making it difficult to read even with an electron-beam microscope.

with a typical lifetime of a few years don't warrant such an effort.

SECURITY ISN'T FREE

Battery packs for consumer devices are cost-sensitive. Ken Dietz, senior applications engineer in Microchip's Security, Microcontroller, and Technology Development Division, suggests that, although battery-pack manufacturers are moving to higher security levels for battery packs, both the size and the price of the circuit still constrain them. "Battery-pack manufacturers ask us: What is the smallest device they can use, what algorithm they can fit onto that device, and how much will it cost to implement the design?" he says. Microchip offers its proprietary KeeLoq algorithm, which the automotive industry has for 10 years used for key fobs. A true encryption scheme, rather than a hashing algorithm, KeeLoq can fit into just 47 code words, allowing the algorithm to fit into Microchip's PIC 10F, which the company claims is the world's smallest microcontroller. In a six-pin SOT-23 package, it costs about 49 cents (volume quantities).

All authentication-IC vendors emphasize that poor security of a company's



Despite being a general-purpose microcontroller, the PIC10F's size and pin count make it a candidate for handling encryption algorithms that can fit into a small block of code. Pin counts range from six (left) to 14 (right).

internal codes can stop the strongest security algorithm in the world. One of Microchip's customers keeps its secret key in an 8x8-ft vault with 3-ft-thick walls, and only two people in the company have vault keys. Gene Armstrong, managing director of thermal and battery management for Maxim, agrees that SHA-1 security depends on keeping the 64-bit key code secure: If someone within the company can steal the key, then no attempts to crack the algorithm are necessary. He explains how the DS2704 security fits into the supply chain: The company ships the part with a programmed, 64-bit key that is not the ultimate secret key. The battery-pack manufacturer assembles the IC into the pack and, as part of the assembly process, issues a challenge to the part and receives a response. The next step in the assembly process is that the process issues a command, "Compute next secret," which becomes the final key the company stores in the pack. "You can implement your supply chain so that no one source has the secret," he says. **EDN**

FOR MORE INFORMATION

Intersil
www.intersil.com
Maxim Integrated Products
www.maxim-ic.com
Microchip
www.microchip.com

Micro Power
www.micro-power.com
Texas Instruments
www.ti.com

MORE AT EDN.COM

For a related article, see "Quantum cryptography: when your link has to be realy, really secure" at www.edn.com/article/CA6290450.

For more on this topic, see "Rolling-code generator uses flash microcontroller" at www.edn.com/article/CA82741.

REFERENCES

- Conner, Margery, "New battery technologies hold promise, peril for portable-system designers," *EDN*, Dec 5, 2005, pg 58, www.edn.com/article/CA6288029.
- Israelsohn, Joshua, "Circuit-protection methods yield more robust products," *EDN*, April 14, 2005, pg 59, www.edn.com/article/CA514947.
- Schneider, Bruce, "SHA-1 Broken," Feb 15, 2005, www.schneider.com/archives/2005/02/sha1_broken.html.
- Friedl, Steve, "An Illustrated Guide to Cryptographic Hashes," www.unixwiz.net/techtips/iguide-crypto-hashes.html.

You can reach
Technical Editor
Margery Conner
at 1-805-461-8242
and mconner@connerbase.com.



TABLE 1 ICs FOR BATTERY AUTHENTICATION

Vendor	Part name	Part no.	Key length	Security algorithm	No. of communication lines	Package supported	Price	Comments
Intersil	Secure authentication IC with Flexihash+	ISL9206	64	Proprietary (Flexihash+)	One	SOT23-5	\$1.15 (1000)	
Maxim	1-kbit ROM	DS2502	NA	NA	One	ThinSOT	Less than 50 cents (1000)	12-byte EPROM
	SHA-1 battery-pack-authentication IC	DS2703	64	SHA-1	Three	2x3-mm TDFN	Less than 50 cents (1000)	
	1280-bit EEPROM with SHA-1 authentication	DS2704	64	SHA-1	One	3x3-mm TDFN	Less than 50 cents (1000)	160-byte EEPROM
Microchip	PIC10F microcontrollers	PIC10F	64 (KeeLoq), 128 (XTEA)	Virtually any algorithm, such as proprietary KeeLoq and open-source XTEA, is software-implementable	One or two	Six-pin SOT-23	49 cents (1000)	
Texas Instruments	Battery-pack-security and -authentication IC	bq26150	128	CRC	One	SC-70	\$1.30 (1000)	96-bit ID plus 16-bit encrypted polynomial and 16-bit encrypted seed; total of 128 bits
	Battery-pack-security and -authentication IC	bq26100	128	SHA-1	Two	SC-70	Less than \$2 (1000)	Introduction in the second quarter of 2006; price is approximate