Keywords: DeepCover, SHA-256, master/slave authentication

APPLICATION NOTE 5779

Introduction to SHA-256 Master/Slave Authentication

By: Bernhard Linke, Principal Member Technical Staff

Jan 22, 2014

Abstract: A new group of secure authenticators and a companion secure coprocessor/1-Wire® master implement SHA-256 authentication. This application note explains the general logistics of this SHA-256-based security system and introduces the bidirectional authentication functionality that the authentication system uses.

A similar version of this article appeared in *EE Times*, June 19, 2013.

Introduction

For more than 10 years, SHA-1 authentication has been used to effectively protect intellectual property from counterfeiting and illegal copying. As computer technology advances, customers are asking for an even higher level of security.

Today a new group of secure authenticators and a companion secure coprocessor implement SHA-256 authentication. This new system provides advanced physical security to deliver unsurpassed low-cost IP protection, clone prevention, and peripheral authentication. This article explains the general logistics of the SHA-256-based security system and introduces the bidirectional authentication functionality which the authentication system utilizes.

A Secure Authentication System

Implementing a secure authentication system requires linking a host system with a sensor/peripheral module. The system presented in **Figure 1** consists of a 1-Wire® SHA-256 secure authenticator plus a SHA-256 coprocessor with 1-Wire master function. Operating between the host and peripheral over a single pin of the 1-Wire interface reduces interconnect complexity, simplifies designs, and reduces cost.[1]

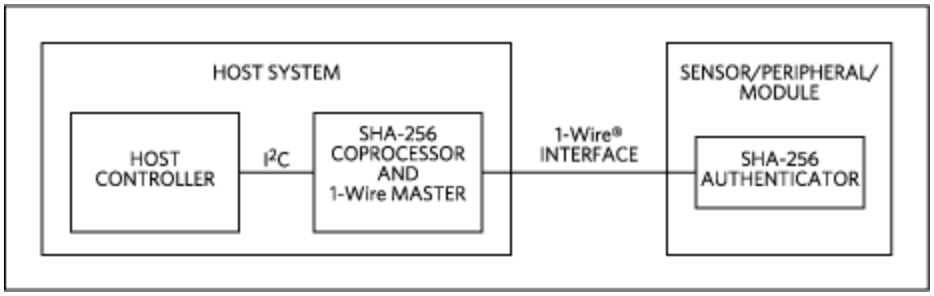

Figure 1. Secure authentication system implementation. This system features the DS2465 SHA-256 coprocessor and the DS28E25 SHA-256 authenticator.

SHA-256 Authenticators

The SHA-256 secure authenticators in this system support a challenge size of 256 bits and use a 256-bit secret. The secure authenticator in Figure 1 is a 1-Wire slave with a unique 64-bit ROM ID that serves as a fundamental data element for authentication computations. The system designer can partition the authenticator's user EEPROM into areas with open (unprotected) access and into areas where the master must authenticate itself for write access. **Table 1** shows the available protection modes and valid protection combinations.

Table 1. 1-Wire SHA-256 Authenticator Protection Options*

Protection Code	Description
RP	Read Protection. If activated, the data is only accessible for device internal use, e.g., like a secret.
WP	Write Protection. If activated, the data cannot be changed.
EM	EPROM Emulation Mode. If activated, individual bits can only be changed from 1 to 0.
AP	Authentication Protection. If activated, write access to the memory requires master authentication.

*The system default is no protection with RP, WP, EM, and AP not activated. Protection is cumulative.

SHA-256 Coprocessor with 1-Wire Master

The SHA-256 coprocessor in Figure 1 is an I²C slave controlled by a host processor. From the host's I²C port the SHA-256 coprocessor appears as a 256-byte read/write memory with certain regions (data elements) assigned for special purposes.

Security Logistics

SHA-based security relies on message authentication codes (MACs) computed from open data and a secret. To verify authenticity, both sides, i.e., the host or coprocessor and the 1-Wire authenticator, must know the secret, which shall never be exposed. Moreover, for maximum security the secret in each 1-Wire authenticator must be unique. In this way the security of the entire system is not affected if the secret of a

single authenticator is ever compromised.

At first glance, it may appear impossible to meet these requirements. There is, however, a simple solution: compute the secret from known "ingredients" and install it into the device in a trusted/controlled manufacturing environment. The ingredients for an authenticator secret are a master secret, the binding data, a partial secret, the authenticator's ROM ID, and padding/formatting ("other data"). **Figure 2** illustrates the process. Although the ingredients are exposed at one point in time, for example, in a trusted manufacturing environment, the computed secret is never exposed and always remains hidden.

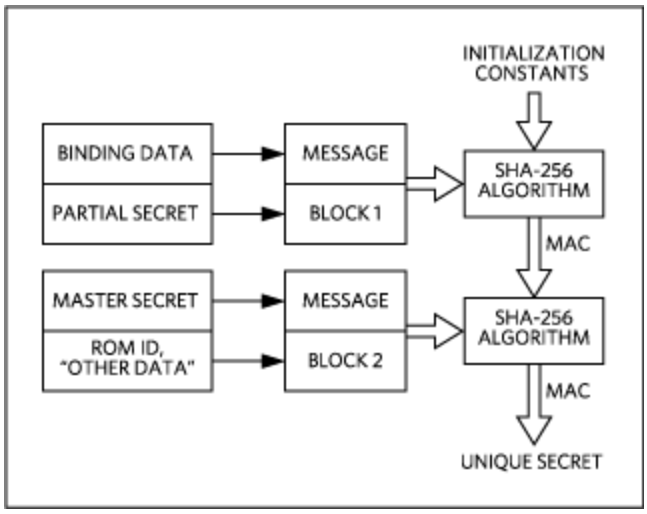

Figure 2. Creating a unique authenticator secret.

For security and storage space reasons, the unique secrets of all authenticators in a system cannot be stored in the coprocessor or host. Instead, the coprocessor stores only the master secret and the binding data in a protected memory section. The partial secret is a system constant that can be coded in the host processor's firmware and communicated openly. After having read an authenticator's ROM ID, the coprocessor can compute the authenticator's unique secret, as shown in Figure 2. With both authenticator and coprocessor now sharing the unique authenticator secret, the system is ready to operate.

Challenge-and-Response Authentication

The primary purpose of an authenticator is to furnish proof that the object to which it is attached is genuine. Symmetric key-based authentication uses a secret key and the to-be-authenticated data ("message") as input to compute a MAC. The host performs the same computation using the expected secret and the same message data; it then compares its version of the MAC to the one received from the authenticator. If both MAC results are identical, the authenticator is part of the system.

In this SHA-256 authentication system, the message is a combination of host challenge and data elements stored in the authenticator. It is crucial that the challenge is based on random data. A never-changing challenge opens the door to replay attacks using a valid, static MAC that is recorded and replayed instead of a MAC that is instantly computed.

The authenticator computes a MAC from the challenge, the secret, memory data, and additional data that together constitute the message (**Figure 3**). If the authenticator can generate a valid MAC for any

challenge, it is safe to assume that it knows the secret and, therefore, can be considered authentic.

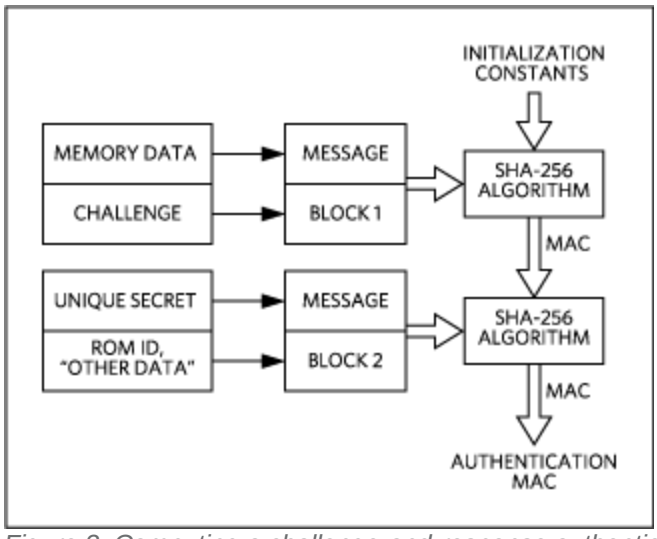

Figure 3. Computing a challenge-and-response authentication MAC.

Data Security (Authenticated Write)

Beyond proving authenticity, it is highly desirable to know that the data stored in the authenticator can be trusted. For this purpose, some or all of the EEPROM in a secure authenticator can be "authentication protected." With authentication protection activated, memory write access requires that the host presents proof of its authenticity by providing a host authentication MAC to the authenticator (**Figure 4**).

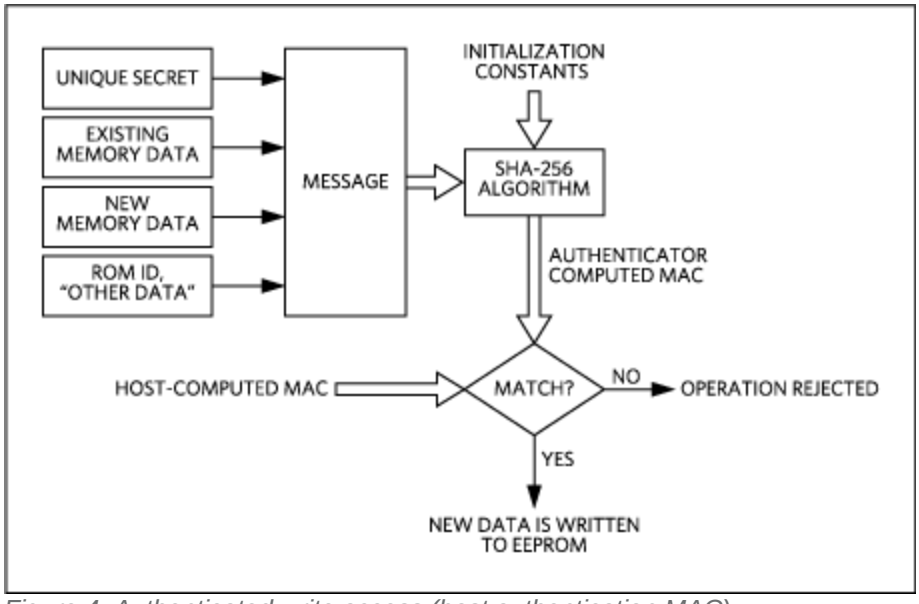

Figure 4. Authenticated write access (host authentication MAC).

The host authentication MAC is computed from the new memory data, the existing memory data, the authenticator's unique secret plus ROM ID, and other data that together constitute the message. The

authenticator computes a MAC in the same way, using its secret.

An authentic host has recreated the authenticator's secret and can generate a valid write-access MAC. When receiving the MAC from the host, the authenticator compares it to its own result. Data is written to the EEPROM only if both MACs match. User memory areas that are write protected cannot be modified, even if the MAC is correct.

Secret Protection

The authenticator's secret and the coprocessor's master secret are read protected by hardware design. If desired, the secrets can be write protected, which prevents tampering with the authenticator's memory data by replacing unknown secrets with known secrets. After installation, the binding data, which is typically stored in the coprocessor's memory, should be read protected. This level of protection is effective as long as the coprocessor and authenticator are set up for the application at a trusted production site.

DeepCover

The deployment of DeepCover® technologies provides the strongest affordable protection against any die-level attacks that attempt to discover the secret key. DeepCover technologies include numerous circuits to actively monitor for die-level tamper events, advanced die routing and layout techniques, and additional proprietary methods to counter the sophisticated capabilities of attackers.

Bidirectional Authentication

The secure authenticators in the example system here support both challenge-and-response authentication and authenticated writes (host authentication). The entire user memory can be used for challenge-and-response authentication. Bidirectional authentication applies to memory areas configured for secure data storage (authenticated write).

Summary

With 256 bits each for the secret, challenge, and MAC, SHA-256 is a significant improvement over older SHA-1 authentication. This article presented a modern, secure authentication system that matches a host system (a SHA-256 coprocessor with 1-Wire master) with a sensor/peripheral module (the 1-Wire SHA-256 authenticators). The coprocessor's built-in 1-Wire master relieves the host from performing 1-Wire communication in real time. DeepCover 1-Wire SHA-256 authenticators are available in three memory configurations for 3.3V and 1.8V operation.[2, 3] Also available for 3.3V and 1.8V, the coprocessor/master[4, 5] works with all three authenticators. SHA-256 security has never been easier.

References

1. A general introduction to mutual authentication is found in Maxim Integrated application note 3675, "Protecting the R&D Investment with Secure Authentication."
2. Maxim Integrated data sheets DS28E15, DS28E22, DS28E25 for 3.3V operation.
3. Maxim Integrated data sheets DS28EL15, DS28EL22, DS28EL25 for 1.8V operation.

4. Maxim Integrated data sheet DS2465 for use with DS28E15, DS28E22, DS28E25.
5. Maxim Integrated data sheet DS24L65 for use with DS28EL15, DS28EL22, DS28EL25.

Related Parts		
DS2465	DeepCover Secure Authenticator with SHA-256 Coprocessor and 1-Wire Master Function	Free Samples
DS24L65	DeepCover Secure Authenticator with SHA-256 Coprocessor and 1-Wire Master Function	Free Samples
DS28E15	DeepCover Secure Authenticator with 1-Wire SHA-256 and 512-Bit User EEPROM	Free Samples
DS28E22	DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb User EEPROM	Free Samples
DS28E25	DeepCover Secure Authenticator with 1-Wire SHA-256 and 4Kb User EEPROM	Free Samples
DS28EL15	DeepCover Secure Authenticator with 1-Wire SHA-256 and 512-Bit User EEPROM	Free Samples
DS28EL22	DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb User EEPROM	Free Samples
DS28EL25	DeepCover Secure Authenticator with 1-Wire SHA-256 and 4Kb User EEPROM	Free Samples

More Information
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact

Application Note 5779: http://www.maximintegrated.com/an5779
APPLICATION NOTE 5779, AN5779, AN 5779, APP5779, Appnote5779, Appnote 5779