SHAMROCK: Self-contained High Assurance MicRO Crypto and Key-management Processor
Technology #15641

Applications

This technology is a self-contained cryptography and key-management solution that is applicable to any crypto-based system or device, and especially suited for applications with strict size, weight, and power restrictions.

Problem Addressed

Traditional cryptographic schemes typically “scramble” or “unscramble” information using a data-permutation algorithm and a short cryptographic key. These keys need to be carefully crafted and managed to preserve the security of the scheme. Although many cryptographic schemes have been standardized and implemented efficiently in software and hardware, they are not universally available due to the lack of broad solutions for key management and the challenge of integrating various cryptographic and key management components into a holistically secure design. To address this issue the Inventors developed SHAMROCK, a self-contained, integrated general-purpose design for a cryptography and key-management solution.

Technology

The design can be realized as an integrated circuit core or an application-specific integrated circuit core. Using a simple, accessible interface, a device containing SHAMROCK chip can use the SHAMROCK’s cryptographic components, such as an Advanced Encryption Standard (AES) cipher core, to secure its data internally and to protect its communication with other devices. The device can also use SHAMROCK to handle all of the key management tasks required for the operation of the cryptographic components. All of these components are integrated in a self-contained, secure design, thereby simplifying the task of incorporating cryptographic protections into applications. SHAMROCK achieves high performance, low power, flexibility, and extensibility by implementing typically computationally demanding components, such as the standard cryptographic functions, directly in hardware.

Additionally, SHAMROCK assures security by separating its internal design into a number of physical regions, and tightly the flow of information from one region into another. It has a dedicated region for storing and handling cryptographic keys. To prevent these keys from leaking, the only physical paths from these regions to those that interface with the application go through a “scrambler” function (e.g. a secure hash function).

Advantages

- Novel technology offers self-contained and centralized key-management solution
- High-performance, power-efficient design
- Restricted physical connectivity completely preserves system security

255 Main Street, room NE 18-501
Cambridge, MA 02142-1601
Phone: 617-253-6966 Fax: 617-258-6790
http://tlo.mit.edu
Contact the Technology Manager: tlo-inquiries@mit.edu
Categories For This Invention:

Computer Sciences & Information Technology
Cyber Security
Lincoln Laboratory
Materials
Polymers (Materials)

Intellectual Property:

Cryptography and key management device and architecture
US Patent Pending
2015-0381659
Cryptography and key management device and architecture
Issued US Patent
9,705,854
Cryptography and key management device and architecture
US Patent Pending
2015-0381592

Inventors:

Roger Khazan
Joshua Kramer
Daniil Utin
Mankuan Vai
David Whelihan

Publications:

SHAMROCK: A Synthesizable High Assurance Cryptography and Key Management Coprocessor
Military Communications Conference
2016, pp. 55-60

External Links:

Lincoln Laboratory
http://www.ll.mit.edu/

Image Gallery: