A Method for Securing Data Using Hardware Functional Gates
Technology #15647

Applications

This technology is a method to secure sensitive data in hardware systems and can be used broadly across all cryptography-based systems to provide higher security by preventing leaks.

Problem Addressed

Modem cryptographic systems are constructed to secure data from eavesdropping and manipulation by untrusted parties, while still allowing trusted parties access to the data. Robust, well understood algorithms such as the Advanced Encryption Standard (AES) are widely used to secure data. However, there are many hardware and software implementations of these algorithms, each of which may have exploitable vulnerabilities given the right level of access. The present invention addresses this problem by applying cryptographic algorithms to ensure sensitive data cannot be steered to a location where it can be extracted by unauthorized parties.

Technology

This is achieved by creating physically separate security zones in hardware systems without direct access from one zone to another. These zones are inter-connected by a number of well-defined Hardware Functional Gates (HFGs), which are cryptographic functions that modify data as it moves from one zone to another. Communication only occurs if data passes through these gates and is sufficiently modified in such a way that it is impossible to recover the original data if the user is unauthorized. For example, data passing from physical zone A to physical zone B must traverse an AES encryption hardware gate, which modifies the data based upon a key held in Zone A. Zone B cannot reasonably understand the encrypted data, but it can move it to another zone. If the data passes back to zone A (within the same or another device), it can pass through a separate HFG that implements AES, and be transformed into its original form, provided the correct hardware decryption key is used. The hardware keys that are used to modify the data passing between zones can only exist in unmodified states in the original zone. If no data value can be known outside of a secure zone, then it is impossible for the cryptographic key to leak, as it will need to pass through an AES functional gate using some value already in zone A, which cannot be known. The security of such a system is provable because the destination of all moving data can be traced through well-defined transformative HFG.

Advantages

- Technology makes it impossible to access data in crypto-system unless authorized.
- Systems with provable security properties can be constructed even when the particulars of a downstream application are not known.
Categories For This Invention:

Computer Sciences & Information Technology
Cyber Security
Lincoln Laboratory

Intellectual Property:

Data security using inter-zone gate circuits
Issued US Patent

Inventors:

Roger Khazan
Joshua Kramer
Daniil Utin
David Whelihan

External Links:

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

Image Gallery: