WHITE PAPER

Carlos Betancourt
Marketing Manager,
Sitara™ processors

Amrit Mundra
Security Architect & System Engineer,
Sitara processors
Texas Instruments

Texas Instruments

Enable security and increase chip performance with hardware-accelerated cryptography

Overview

In 2014, an estimated 17.6 million Americans experienced identity theft victimization, according to the Bureau of Justice Statistics. The list of security risks continues to grow when adding hacking, phishing, malware and viruses. In today's hyper-connected world, the opportunities to be victimized by a scam or theft are a mouse click or a tap on a touch screen away. Important personal and confidential information is placed on the Internet and sent across wireless connections constantly by millions—if not billions—of people every day.

Cryptography, the science of obfuscating or hiding information to prevent it from falling into the wrong hands, has become extremely critical for all electronic devices. From personal computers to wireless mobile devices and even embedded processors deployed in a myriad of end-user applications such as industrial controls, residential automation and home entertainment centers, technology has enhanced user experiences. With more proficiencies, however, manufacturers of every electronic device must come to terms with the issue of security.

Given the general public's preoccupation with it, failing to incorporate the proper security measures into a new product can cause its demise in the marketplace. Moreover, how security is implemented is often just as crucial to a product's success. The processing of complex cryptographic algorithms can be taxing for many processors, making the device or system seem unresponsive and sluggish and diminishing its user experience. Manufacturers must manage the tradeoffs: How to deploy the level of security needed to reassure users without slowing down the device to the point where the user experience is affected?

With TI's Sitara™ embedded processors—specifically, the AM37x, AM335x, AM43x and AM57x devices—manufacturers can avoid this tradeoff. Accelerating cryptographic processing in hardware instead of performing these algorithms entirely in software ensures that security measures do not get in the way of an engaging and satisfying user experience.

Cryptography basics

Cryptography is one of several techniques or methodologies that are typically implemented in contemporary electronic systems to construct a secure perimeter around a device where information or digital content is being protected. This data must also be safeguarded when it is communicated outside of the device. Other types of security measures such as secure boot code and run-time security are different sorts of security techniques from cryptography. This white paper is focused on cryptography, one of several methods which are employed in security subsystems.

The word cryptography comes from the Greek meaning "hidden" or "secret writing". On the most basic level, it is concerned with encoding or encrypting communications to keep the meaning hidden from everyone except those who are authorized of decoding or decrypting it. As such, cryptography involves a set of communication protocols often based on higher order mathematics. On one side of a communication channel, data is encrypted before it is transmitted. The receiving end will possess the decrypting algorithms so the data can be transformed back into a readily understandable form.

In contemporary computer and communication systems, cryptography is employed to secure data and achieve four purposes

1. Confidentiality – Ensure that an asset is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.

2. Authentication – Ensure that assets or entities (i.e., data, transactions, communications, software or documents—electronic or physical) are genuine and authorized to perform a task or be used as they are intended to be. Validate that all parties involved are who they claim to be.
3. Data integrity – Protection of assets from unauthorized modification.
4. Non-repudiation – When an individual takes responsibility for an action, such as a commitment to purchase something, that commitment cannot be denied or repudiated at a later time.

These different purposes for data security figure prominently in a wide variety of end-user applications deployed extensively all over the world, including Web browsing, e-commerce, secure wireless communication links, virtual private networks (VPN) and many others.

Building on security

Typically, system designers decide which security tools they will use to build a security sub-system. In all likelihood, such a subsystem will include cryptography. Many embedded systems are based on the Linux® open-source operating system. There are a number of specialized security frameworks that can be implemented in Linux systems. In addition, several open-source cryptographic algorithms will plug into these security frameworks and provide them with cryptographic capabilities. Here are a few:

1. Specialized security frameworks

Some of the most prevalent open-source security frameworks include the following:

- OpenSSL – Implements two secure communications protocols, the Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols.
- WPA Supplicant – Implements the IEEE 802.11i security mechanisms for wireless local area networks (Wi-Fi®).
- Dropbear – Implements a secure server and client.
- OpenSSH – Implements a secure server, client and file transfer protocol (FTP) server.
- Cryptodev – Cryptodev-linux is a device that allows access to Linux kernel cryptographic drivers; thus allowing of user-space applications to take advantage of hardware accelerators

2. Cryptographic algorithms

Some of the common cryptographic algorithms which are integrated into security applications are the following:

- Data Encryption Standard (DES) – The DES encryption algorithm was developed in the 1970s. Although it has been widely deployed over the years, it has subsequently been superseded by other algorithms.
- 3Data Encryption Standard (3DES) – 3DES performs DES encryption three times to strengthen the protection of the encrypted data and overcome some of vulnerabilities of the DES algorithm.
- Advanced Encryption Standard (AES) – AES is one of the most advanced cryptographic algorithms in widespread use today.

3. Hashing functions

Another type of cryptographic algorithm is known as "hashing" or a "hash function." A hash function is applied to data to create a hash value or "digest". Surreptitious or accidental changes to the data will change the hash value. Hashing is particularly useful in certain cryptographic operations such as digital signatures, data integrity, non-repudiation, message authentication and other forms of authentication. Several hashing algorithms have been standardized and are in common use today, including the following:

- Message Digest Algorithm (MD5) – Although this hashing function has been widely deployed, it has certain vulnerabilities in some applications.
- Secure Hash Algorithm (SHA) – SHA has gone through several generations, SHA2 is commonly used. SHA3 is new standard for hashing.

4. Random number generators

Another important aspect of many security applications is a random number generator. Random numbers are used by several of the functions which comprise a security subsystem, including encryption algorithms and hashing functions. It should be noted that random numbers generated in software are not always true random numbers. Hardware-generated random numbers are more often truly random.

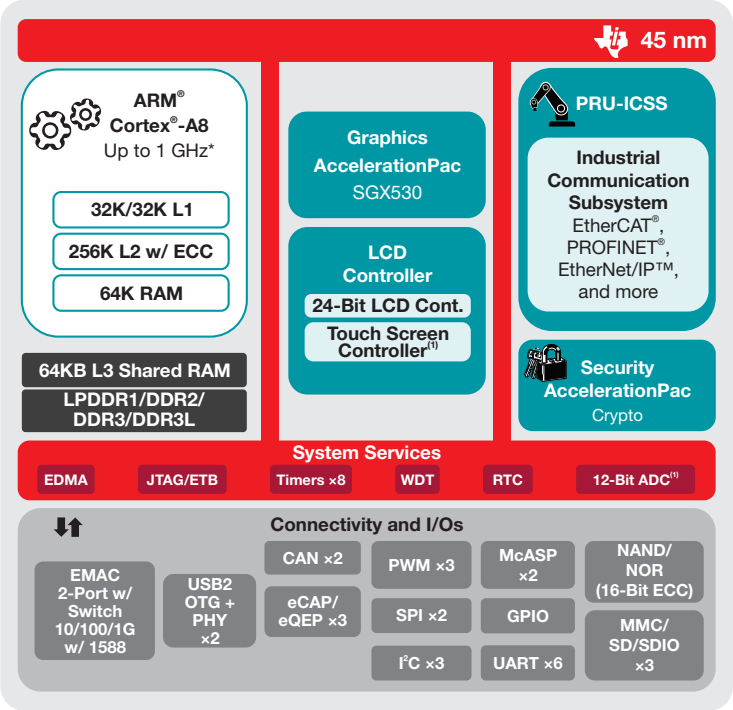
5. Hardware acceleration vs. software execution

How and where cryptographic algorithms are processed is another important consideration for developers. Saddling the system's main CPU with the burden of processing computationally-intense cryptographic code will siphon processing cycles away from the system's user applications and possibly detract from the user experience. Some embedded processors, such as several of TI's Sitara devices (see the table on page 5), have been equipped with hardware-based accelerators dedicated to cryptographic processing. These specialized accelerators offload the bulk of the cryptographic processing from the system's CPU so that the CPU's processing bandwidth is retained for end-user application processing. As a result, the overall throughput of the system is optimized.

Cryptography on TI Sitara Processors: Moving from software to hardware implementation

TI has extensive experience supporting cryptography on its Sitara processors, which are based on ARM Cortex®-A8, -A9 and -A15 cores. Developers have been able to take advantage of the OpenSSL and Cryptodev security framework on Sitara processors since 2009. OpenSSL and other cryptographic algorithms executed in software on the ARM core, until early 2011 when hardware-based accelerators were introduced with the AM37x. These hardware accelerators operate separately from the ARM core so that when cryptographic security processing is required, it does not steal processing cycles away from the ARM core. That is to say that almost all of the cryptographic processing is offloaded from the ARM to distinct security accelerators elsewhere in the hardware. This offloads the processing of computationally-intense security algorithms from the ARM core, retaining processing cycles on the ARM for those tasks it is particularly well suited to perform,

such as operating system housekeeping tasks, the user interface, graphics, the Wi-Fi wireless communications stack, control software and most application software. (See Figure 1. Sitara AM335x processor block diagram below.)



** 800 MHz / 1 GHz only available on 15×15 package. 13×13 supports up to 600 MHz.*

(1) Use of TSC will limit available ADC channels.

Figure 1. This block diagram of a Sitara AM335x Cortex®-A8 processor highlights the hardware-based security accelerators that offload cryptographic processing from the ARM core.

This shift to a more effective method of cryptographic processing has been accomplished seamlessly and in a manner that is transparent to developers. When executing security algorithms in the past, the ARM core would call a security API, and the required algorithm would be processed on the ARM. Now, with separate hardware-based security accelerators, the ARM still calls the same security API, but the subsequent processing of the security algorithm now takes place on the distinct hardware accelerator module, not on the ARM. Since the ARM acts in the same way with regards to the security API, shifting cryptographic processing from the ARM to a separate hardware module has limited effects on the rest of the system's software.

Tests have demonstrated that hardware-based cryptographic acceleration of OpenSSL can lower the CPU utilization by as much as 50 percent. This has far-reaching effects on the ARM core's processing bandwidth. In fact, developers might contemplate utilizing this new-found processing headroom for enhancing the user experience with exciting application features that previously could not be supported.

The table below lists the specific cryptographic algorithms supported by the AM37x, AM335x, AM43x and AM57x Sitara processors.

	Cryptography Algorithms				
Sitara processor:	**AES**	**DES/3DES**	**MD5**	**SHA**	**True RNG**
AM37x	✔	✔	✔	✔	
AM335x	✔		✔	✔	✔
AM43x	✔	✔	✔	✔	✔
AM57x	✔	✔	✔	✔	✔

Tooling up for security

Deploying a cryptographic security sub-system on one of the Sitara processors is supported by a multi-layered tools environment. Evaluation modules (EVM) featuring these devices are readily available and ready to use, right out of the box. Soon after powering on an EVM, hardware and software engineers can download software modules and begin developing the system's security environment with tools available in the device's Software Developer Kit (SDK).

The Processor SDK for the Sitara AM37x, AM335x, AM43x and AM57x processors is an online toolkit from which executable cryptographic modules can be run via a slick interface, similar to the one on a smartphone (Figure 2). The Processor SDK interface can also be featured on the touch-screen panels of those EVMs featuring a screen attached to the board. OpenSSL with several of the prominent cryptographic algorithms, as well as extensive documentation are available in the Processor SDK. For example, the OpenSSL speed test is one of the tools in the Processor SDK and provides performance results for all available algorithms. This gives developers a metric for comparing alternative security implementations under OpenSSL.

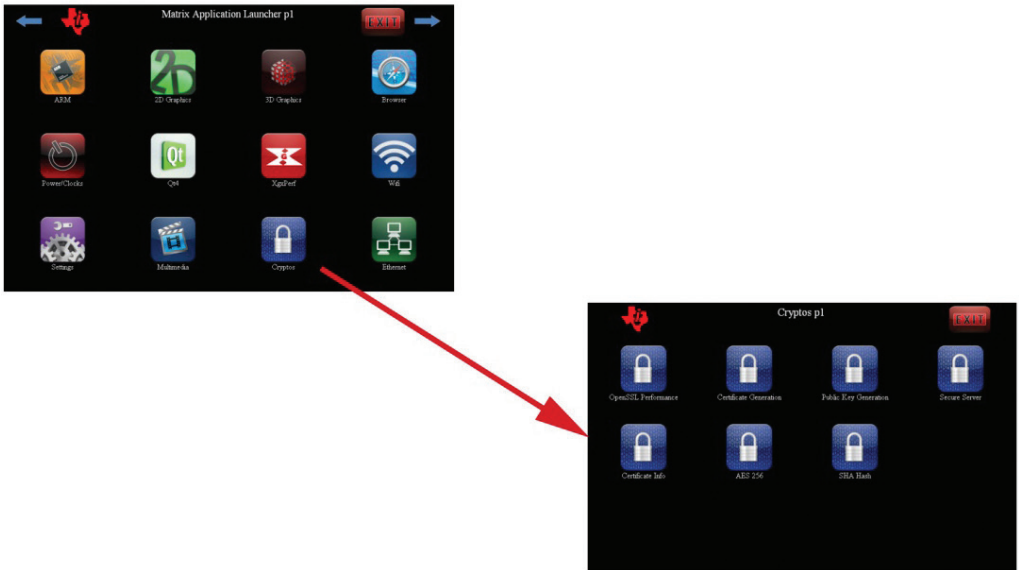


Figure 2. Selecting the "crypto" icon on the Processor SDK on the left will take a developer to the cryptographic modules for testing.

Engaging the Sitara processor hardware acceleration module for cryptographic processing can be completely transparent to developers. The OpenSSL driver for the Sitara processors automatically directs cryptographic processing to the hardware acceleration module with no intervention on the part of developers. Unless explicitly directed by developers, OpenSSL security applications are executed on the hardware acceleration module.

Making a difference

Differentiating features or capabilities which make a product stand out in the marketplace can come from various sources. Top-notch cryptographic security protection might distinguish one system. Another might receive a lot of buzz for an enhanced user application or feature not found on competing products. The hardware-based cryptographic acceleration of the Sitara AM37x, AM335x, AM43x and AM57x processors makes both of these possibilities probable. In all likelihood, cryptographic algorithms will execute more effectively when they are processed by a hardware module dedicated to security rather than being processes as just another piece of software running on the system's main CPU. Offloading the cryptographic processing from the ARM core also gives developers the processing headroom they need to create the next great enhancement the market is looking for. Both the user and the manufacturer end up as winners.

For more information, please visit **www.ti.com/sitara**.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265