# A Method of Data Storage and Management of Embedded Trusted Platform Module

**Gang Liu, Xun Zhang, Yuan Zhang**
School of Computer Science and Technology, Xidian University, Xi'an 710071, China
gliu@xidian.edu.cn

**Abstract** - This paper firstly discusses the data storage and management of trusted platform module (TPM) system on a trusted PC, mainly including certificates and keys, platform configuration registers (PCR), and firmware program. In order to overcome the limitations of TPM defined by Trusted Computing Group (TCG) and resolve the differences between the embedded platforms and the PC platforms, on the basis of prototype system architecture of embedded trusted computing chip based on System on a Programmable Chip (SOPC), the paper explores the data storage and management of embedded TPM emphatically. Finally, a data storage and management method of embedded TPM system which carries on the problems of embedded devices is designed.

**Index Terms** - SOPC, Embedded, Storage and Management, TPM

## 1. Introduction

With the continuous development and progress of science and technology, embedded technology is developing rapidly. With the wide application of embedded system, it is also growing that the attacks of hardware and software [1]. Compared with the PC, embedded system is mainly faced with many security challenges. The species of security threats are becoming more and more complex to the embedded products, so it has reached the point of the urgent to solve the existing security problems of embedded systems. The United States set up the Trusted Computing Platform Alliance in 1999, and the group changed its name to the Trusted Computing Group in 2003. The core technology of TCG mechanism is the TPM [2] which is a small System-on-Chip containing cryptographic computation units and storage units. The TPM has strong anti-interference which can be used as a root of trust for service [3] [4].

In this paper, we present the data storage and management structure on the basis of the embedded trusted computing chip system architecture after the research of the TPM specifications and the SOPC method. In the second chapter of this article introduces the design work foundation briefly, and the third chapter describes the design of data storage and management structure in detail.

## 2. Work Foundation

Trusted computing technology, which is adding hardware security features on the PC hardware platform, and improving the terminal system security by providing security features. "Trusted Computing" contains the hardware measure of security, the secure data storage and the platform and user authentication security function [5]. Trusted Platform Module (TPM) is the trusted root of the trusted computing platform, and it is the core module of trusted computing. TCG defines the TPM standard of secure storage and encryption function. TPM chip is a complex System-on-Chip, which not only has execution engines, but also integrates many cryptographic computation modules, and all cryptographic operations are performed in the TPM chip [6]. TPM specification defines the algorithm modules and functions that must support in detail, and Fig. 1 shows the composition structure of the TPM chip.

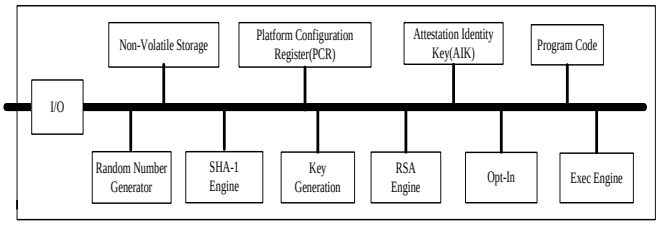


Fig. 1 TPM Component

With the development of FPGA technology, FPGA logic capacity is higher, while the cost is lower. With this trend, the FPGA could replace more and more devices in the system, and develops into the FPGA System-on-Chip eventually. Xilinx introduces the 32bit Micro Blaze soft-core, it can be changed according to the design demands and completes the design requirements with the least resources.

To sum up, Fig. 2 shows the work foundation [7] of this article: prototype system architecture of embedded trusted computing chip. It combines with the characteristics of the TPM architecture of TCG and the Xilinx FPGA embedded System-on-Chip and all of its modules are implemented in the form of flexible IP core, through the system bus integrate to the microkernel controller, eventually form a complete SOPC system. Meanwhile Xilinx FPGA embedded System-on-Chip can also to construct a system of multi-core processor.

The system includes five parts: the storage unit; the operation unit; the I/O interface; the control unit; the system bus. The storage unit is used to store data which are needed for TPM implementation and operation. The operation unit is used to generate and process data for TPM required and ensure the safety of the system operation. The I/O interface is used to connect the TPM and embedded devices. The control unit is used to control and manage the TPM's various operations. The System bus is a bus access to system resources.

This paper describes the design of the storage unit and the

relevant parts of the control unit in detail on the basis of the SOPC system architecture above, so as to realize storage and management of the system internal data.

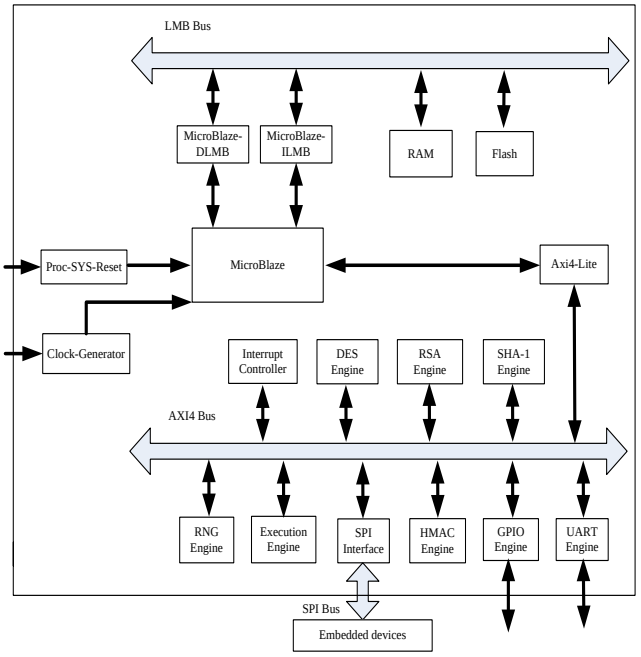


Fig. 2 Structure of Reconfigurable TPM

## 3. Design of Storage and Management

### *A. TPM Data Storage and Management of Trusted PC*

According to the TCG standards [8], TPM data can be classified into volatile and non-volatile data by the presence of the data. The data also can be classified into credentials and keys, PCR data, firmware program and other data by the type of required data. The secure data storage provided by TPM is used to protect the data security and privacy. TPM stores sensitive data in the internal shielding area of the chip, and the system's other secure data are stored in the external storage devices after encryption by the storage key. This part will mainly introduces the TPM data storage and management system based on trusted PC, respectively from three aspects of credentials and keys, PCR data, and firmware program.

#### *1) Credentials and Keys*

TCG standards define five types of credentials: endorsement credential, conformance credential, platform credential, validation credential and identity credential. The attestation of the platform can be completed with these credentials together, and Fig. 3 shows the relationships between the credentials.

Meanwhile, TCG standard also defines seven types of keys: endorsement key that is used to decrypt the owner's authorization data and generate data associated with AIK; identity key is used to sign the data generated by the TPM; signing key is used to signature on the application data and information; storage key is used to encrypt data or other keys; bind key is used to encrypt small-scale data that will be decrypted on another TPM platform; legacy key which is created outside the TPM and will be imported into TPM when it is used for signature and encryption; authentication key is used to protect the transmission session which cited TPM. According to the TCG standards, endorsement key and storage root key as the non-volatile data in TPM are never exposed to the outside of the TPM, while the others encrypted with the storage key are stored in the external storage devices outside the TPM. When we need to use these keys, we can reload them to the TPM.

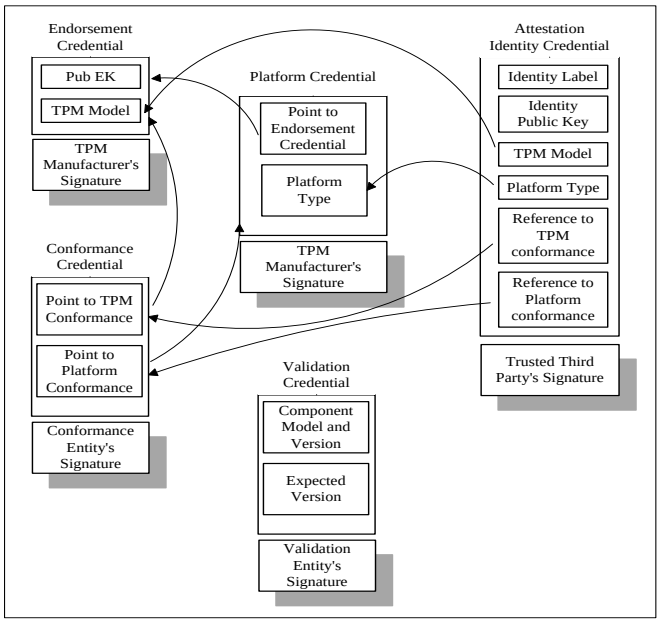


Fig. 3 Credentials and their Relationships

#### *2) PCR Data*

Platform Configuration Register (PCR) is a 160 bits storage unit for storing the platform integrity measurement information. According to the TCG standards, the TPM should have 16 PCR registers at least. All PCR registers are stored in the TPM protected region. Generally, a typical PC system has 24 PCR registers, and each register stores a particular hash value. PCR[0...7] for system startup, TCG specification defines their specific usage in detail. PCR[8...15] are used by the operating system, and the last 8 PCR registers are provided for dynamically accessed devices.

In the TPM based on trusted PC, PCR data are stored in a volatile memory in the TPM usually. When the system is powered on, all the software must be measured and stored before execution. As the system start-up and the transfer of trust chain, it measures the various modules and saves the integrity measured data. Regardless of the state of the platform, measured data kept in a PCR register can report platform information correctly.

#### *3) Firmware Program*

The trusted root must be a trusted component in the TPM system. There are usually three public trusted roots in a trusted computing platform: root of trust for measurement (RTM),

root of trust for storage (RTS) and root of trust for reporting (RTR). The RTM is a computing engine capable of making inherently reliable integrity measurements. Generally speaking, the platform computing engine is controlled by the CRTM. The CRTM is the first piece of code executed by the trusted platform when it starts up. With CRTM as a starting point, Trusted Computing Platform measures the integrity of the entire platform resources by trusted chain, and stores the information in the TPM's Platform Configuration Registers. The trusted chain, BIOS Boot Block and the TPM chip as trusted roots, through the credible reports submitted by constantly trusted measurement, can get to know the credibility of the platform by matching entity measurement information with the expected information. The CRTM in PC architecture is usually stored in external non-volatile memory which is as shown in Fig. 4.

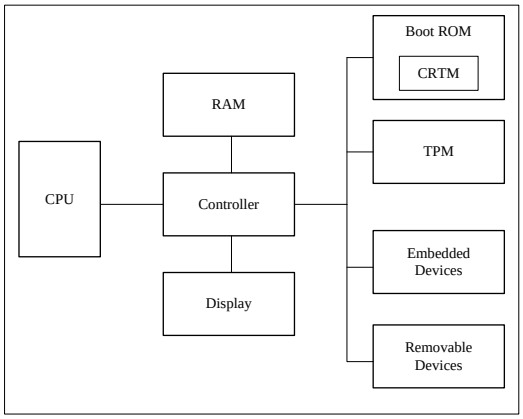


Fig. 4 Trusted Platform Components

*B. TPM Data Storage and Management of Trusted Embedded Device*

The design of TPM data storage and management of trusted PC has strong characteristics of the PC, there will be many problems if the data storage and management design based on the trusted PC directly transplanted to embedded devices system, such as the phenomenon that mismatching between the requirements of safe and the available processor processing capacity leads to embedded devices cannot run. Taking into account the small kernel, strong specificity, streamline and other characteristics of the embedded device system, this paper proposes a data storage and management architecture of trusted embedded TPM based on the SOPC method.

The proposed design in this paper has been done validation on DIGILENT Nexys3 development board. The development environment is Xilinx ISE Design Suite v14.1. Nexys3 development board is a digital system development platform based on the latest technology Spartan-6 FPGA.

*1) Design of Credentials and Keys*

Attestation of trusted platform is accomplished by a series of credentials and keys. TCG specification defines five types of credentials. The specificity and streamline characteristics of embedded devices and the implementation of every credential determine that all of them can't be realized on a embedded device. There are only two credentials, EK credential and AIK credential, used in this design. Fig. 5 shows the structure and relationship of the two kinds of credentials.

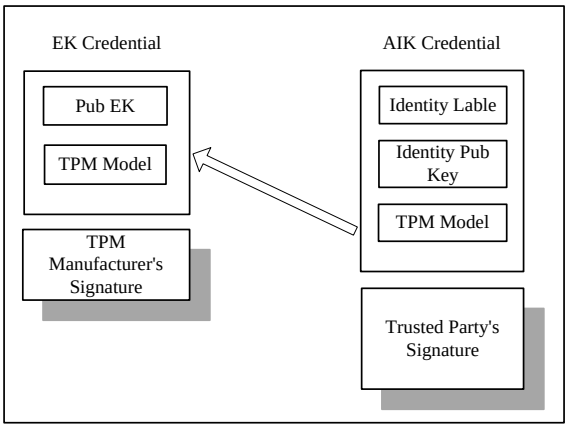


Fig. 5 Structure and Relationship of Credentials

The keys cannot be generated and used without the credentials. With the above two kinds of credentials, the storage and management architecture in this design use four kinds of keys: the endorsement key, identity key, signing key and authentication key. The endorsement and identity key are the focus of keys storage and management among them.

EK credential which exists in a valid TPM generates the only EK key pair to this platform. AIK credential is mainly used to generate the AIK key pairs. Existing as the root key, EK key pair is not generally used to encrypt or sign messages directly with the security consideration, which is the reason why the AIK key pair appears as substitutes for EK key pair. AIK key pairs are only used for signature, and cannot be used for encryption. TPM can theoretically produce arbitrary number of AIK key pairs for signing.

There will not be many available keys by reason of many embedded devices using relatively single characteristic, so all of the keys can be stored inside the TPM in design. Endorsement key is stored in a protected area within the TPM, which is the non-volatile memory. Identity key, the signing key and the authentication key are dynamically generated after the TPM starting. When we restart the embedded TPM, identity key, signing key and authentication key are regenerated while endorsement key remains unchanged. Keys are generated using random Numbers which are generated by a true random number core within the TPM. This greatly improved the security of the system.

*2) Design of PCR Data and Firmware Program*

PCR value is a sign to mark a machine state, no matter it can be trusted. The PCR registers are divided into two categories, one kind is used for embedded system boot-up, and the other one is used for the operating system applications and dynamic access devices. The CRTM is stored in non-volatile memory of embedded TPM to ensure the integrity and security

in this design. Trust chain of the platform starts to be established from the CRTM, and the CRTM will complete the rest of the platform integrity measurement in the platform initialization phase. For embedded devices, the whole system boot-up and loading tasks are accomplished entirely by the Boot Loader which is different from the BIOS Boot Block boot-up mode of the trusted PC's TPM. Therefore, the design of the PCR registers are as follows: 16 PCR registers are set in the embedded TPM volatile memory, as shown in Fig. 6.

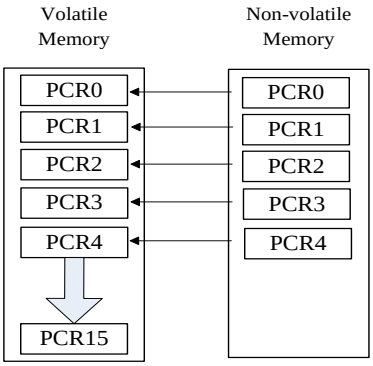


Fig. 6 Design of PCR Registers

We can allocate PCR registers space dynamically, and there be unlimited number of PCR registers in theory. PCR[0] and PCR[1] are used to store Boot Loader information measured data, PCR[2], PCR[3] and PCR[4] are used to store the operating system and other important configuration information measured data. These values are not allowed to be changed and stored in the non-volatile memory. For general embedded devices, these devices operating system and configuration information are once determined, they will not be changed or updated for a long time. When the embedded TPM self-test operation is successful, the result of the comparison between the Boot Loader information integrity measurement and the standard value which is measured data of the Boot Loader information in non-volatile memory loaded into volatile register determines whether the Boot Loader's integrity is destroyed or not. If the integrity of the Boot Loader is not damaged, then the Boot Loader can be started. After the Boot Loader starting up, then the operating system and configuration information values in the non-volatile memory will be loaded into the volatile memory as the standard values, and then the measured data will be compared with the standard values to determine the integrity of the operating system. PCR[5...15] are representing the integrity measurement values which are stored in volatile registers sequentially. After the operating system's successful measuring, we can measure and record applications and access devices on the basis of operating systems. So the chain can pass down in such a simple way, which as shown in Fig. 7.

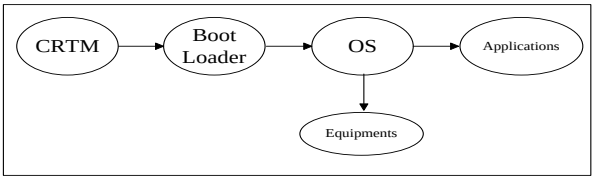


Fig. 7 Transfer of Trust Chain

In addition to the TPM important data mentioned above, there are some flag data and intermediate data stored in the volatile memory of TPM when the system is running. They will not to be introduced in detail in this article.

## 4. Conclusions

With the wide application of embedded systems, the attacks from hardware and software are also growing. At the same time, embedded system faces more and more serious security threats. Trusted computing technology, an emerging technology to building secure computing platform, can be introduced into the field of embedded system to solve the embedded platform security problems. This paper proposes a data storage and management structure on the trusted computing chip prototype system by researching the TCG specification about TPM. Taking the characteristics of embedded system into full consideration, this structure can cope with limited resources of embedded system. Based on the high-speed FPGA environment, the structure has the advantages of high speed, high efficiency and easy to modify and expand. This design provides a reference to other designs about the data storage and management on embedded security chip.

## References


[1] D. Dagon, T. Martin and T. Staner, "Mobile Phones as Computing Devices: The Viruses are Coming!," *IEEE Pervasive Computing*, 2004.

[2] Frederic Stumpf, Michael Benz, Martin Hermanowski, Claudia Eckert, "An Approach to a Trustworthy System Architecture Using Virtualization," *ATC* 2007: 191-202.

[3] TCG, "TCG Trusted Computing Group (TCG) Main Specification (v1.2)," 2011, 1.

[4] Bin Yan, "A Kind of FPGA Implementation of Security Implementation Mechanisms of Trusted Computing Platform," *Computer & Digital Engineering*, vol. 39, no. 9, pp. 110-113, 2011.

[5] Jingchun Fan, "Research and Development of Trusted Computing," 2007.

[6] David Challener, *A Practical Guide to Trusted Computing*, Beijing: China Machine Press, 2009.

[7] Bin He, *AXI4-Based SOC Programmable Systems Design*, Beijing: Tsinghua University Press, 2011.

[8] TCG, "TCG Specification Architecture Overview (v1.4)," 2007.