A Low-Cost Cryptographic Processor for Security Embedded System

Ronghua Lu, Jun Han * , Xiaoyang Zeng, Qing Li, Lang Mai, Jia Zhao
State Key Lab of ASIC and System, Fudan University, Shanghai, 200433, China
Email: 052021062@fudan.edu.cn; junhan@fudan.edu.cn

Abstract—A low-cost cryptographic processor for security embedded system is presented in this paper. The processor, without any assistance of dedicated cryptographic coprocessors, is scalable and very efficient for popular cryptographic algorithms such as RSA/ECC, AES, Hash, etc. Based on SMIC 0.18um standard CMOS technology, the core circuit of the test chip has only about 32k gates, and a max frequency of 200MHz, under which the 1024-bit RSA algorithm takes only 150ms and the throughout of AES reaches 256Mbits/s.

Ⅰ. Introduction

Cryptographic algorithms play an important role in nowadays security system. It is not difficult to implement them completely in software, but such solutions are too slow for real-time applications. Most proposed schemes focus on the SoC (System-on-Chip), which generally consists of embedded CPU and on-chip bus, DMA controller, memories, and some other assistant modules such as dedicated coprocessors for the acceleration of executing these algorithms. However, these accelerators often consume a large part of the expensive chip size and power consumption and are not flexible enough to support software-like flexibility.

In this paper, a scalable cryptographic processor named as CryptoAeg for security embedded system is proposed. Different from other general SoC-based solutions, CryptoAeg has its own powerful cryptographic instructions to accelerate cryptographic processing. These instructions will definitely eliminate the need of coprocessors and thus obviously lower the cost of system.

Ⅱ. Hardware Architecture of CryptoAeg

Figure 1 shows the hardware architecture of CryptoAeg. Different from the typical 32-bit RISC CPU, the processor has not only a common 5-stage pipeline structure but also more than two execution units in particular. In most time, ALU acts as the main execution unit when the processor is running a normal program. However, the special execution units (FU) will take effect when the cryptographic instructions are ongoing.

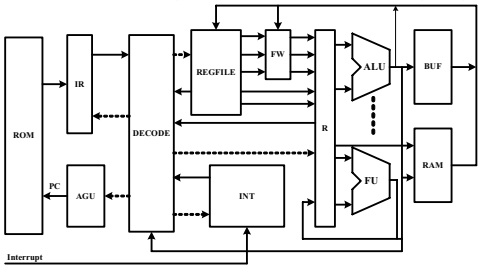

Fig. 1 Hardware Architecture of CryptoAeg

Most proposed cryptographic processors adopt the MAC cell to perform the modular multiplication in RSA or ECC. The design developed in this paper centers on the ALU architecture and does not include any multiplier. Consequently, the hardware cost is reduced and a long critical path of multiplier is eliminated.

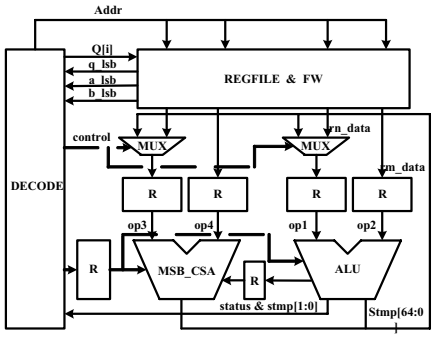

Fig. 2 Main Data Path for Modular Multiplication

The main data path for modular multiplication is illustrated in figure 2. With the help of special addition unit MSB_CSA [3], CryptoAeg executes a 64-bit modular multiplication within 64 cycles, which is achieved by directly forwarding the current computing result to next round as input data. Unlike general RISC CPU, some of the registers are also designed to automatically store parameters produced when cryptographic instructions are executed. So there is no need to calculate these parameters by software, and consequently the complexity of implementing cryptographic algorithms in software is sharply reduced.

Ⅲ. Instruction Extension and Implementation for Security Embedded System

Figure 3 shows the scheme for cryptographic instruction extension of CryptoAeg. The most critical and complicated process of each algorithm is analyzed, and then a special execution unit such as MSB_CSA, AES_FU or FUn is designated to accomplish the process. Those units could be invoked by a set of cryptographic instructions. Thus the programmer can easily implement and configure an algorithm. This method of extension will lower both of the hardware cost and complexity of software program.

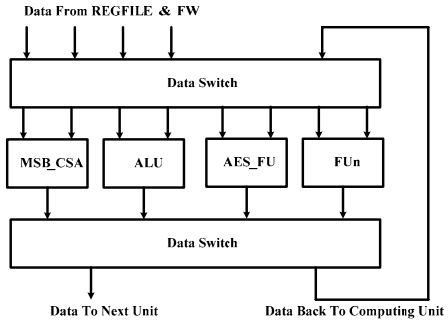

Fig. 3 Scheme for Cryptographic Instruction Extension

Compared with other proposed SoC solutions, several FUn in CryptoAeg share the resources with ALU, so

978-1-4244-1922-7/08/$25.00 ©2008 IEEE

software-like flexibility is completely achieved. This means the configuration of algorithm is totally determined by the programmer.

Figure 4 shows a security embedded system based on CryptoAeg. It includes the following several important modules: the embedded RISC CPU (CryptoAeg), AMBA bus, USB2.0 engine, on-chip memories and some other low-speed devices. The AMBA bus is suitable for connecting all the modules and presents a flexible environment for module's interface and communication.

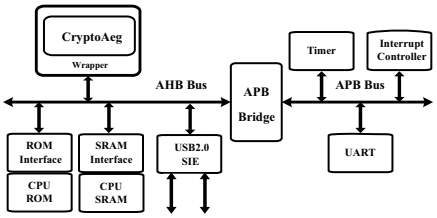

Fig. 4 Hardware Architecture of the Security Embedded System Based on CryptoAeg

Since the system controller CryptoAeg can also execute all the supported cryptographic algorithms, there is no cryptographic coprocessors integrated in the system, leading to the remarkable reduction of system cost and making CryptoAeg very suitable for the low-cost client-end applications of information security, especially for the field of portable devices.

Ⅳ. Implementation and Test Results

Figure 5 shows the die photo of CryptoAeg test chip to realize the architecture in Fig. 4. Based on SMIC 0.18um standard CMOS technology, the total die size is about $4.9788*1.7794mm^2$. The test results indicate that CryptoAeg can work stably at 200MHz. Tab. 1 compares the RSA performance of CryptoAeg with other implementations from ARM, MIPS, and NEC [6,7,8]. CryptoAeg outperforms these implementations by a factor of 4 to 6. As described in Fig. 6, the performance of AES is 256Mbits/s, which is faster than Hifn7854 [9] and is analogous to many other outstanding machines. The test chip has only about 32k core gates and a very low power consumption of about 70mW under 60MHz. Fig.7 is the comparison result of power consumption and core size among CryptoAeg, SecuCore and another SoC-based cryptographic processor SP [5,6].

Since CryptoAeg has no special instruction for Hash, we implement SHA-1and MD5 algorithms completely in software. The result shows that it only takes 0.025ms to execute Hash, and ulteriorly prove that CryptoAeg is sufficient for the low-cost client-end applications of information security.

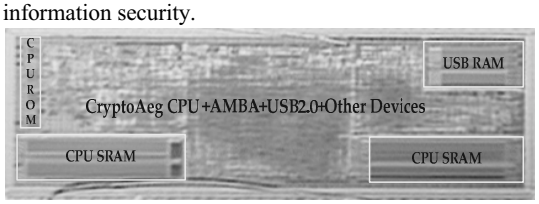

Fig. 5 Die Photo of the CryptoAeg Test Chip

Ⅴ. Conclusions

In this paper, a low-cost cryptographic processor named as CryptoAeg for security embedded system is presented. The test results show that CryptoAeg works well with all the supported algorithms. By its optimized architecture and powerful cryptographic instructions, CryptoAeg has achieved both software-like flexibility and hardware-like performance for the client-end applications of information security such as portable devices and wireless communications.

Tab. 1 Comparison Result of RSA Performance

Company	Product	1024-bit RSA
ARM	Secure Core SC200	594ms
MIPS	SmartMIPS 4KSc	320ms
NEC	V-WAY32 uPD792150C	436ms
Ours	CryptoAeg	150ms

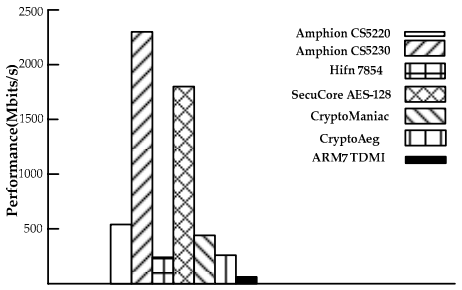

Fig. 6 Comparison Result of AES Performance

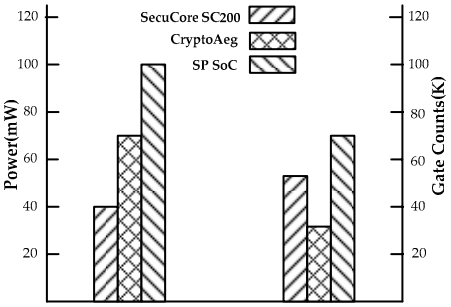

Fig. 7 Comparison Result of Power and Core Size

Reference

[1] Rivest R L, Shamir A and Adleman L A.. "Method for obtaining digital signatures and public-key cryptosystems". Communications of the ACM, 1978, 21(2): 120-126.

[2] Advanced Encryption Standdard, Nov.26, 2001.

[3] Jun Han, XiaoYang Zeng, Ronghua Lu, Jiao Zhao. "Attack-resisted Coprocessor Integrating Multiplication and Inverse". Journal of Chinese Computer System, Vol28, No.4, 2007, page(s): 753-758.

[4] Min Wu, Xiaoyang Zeng, Jun Han, Yongyi Wu, Yibo Fan. "A high-performance platform-based SoC for information security". Design Automation, Asia and South Pacific Conference,2006, Pages(s): 10pp.

[5] Chen-Hsing Wang, Jen-Chieh yeh, Chih-Tsun Huang, Cheng-Wen Wu. "Scalable Security Processor Design and Its implementation". Asian Solid-State Circuits Conference,2005, Pages(s): 513-516.

[6] ARM Limited. http://www.arm.com.

[7] MIPs Technologies, Inc. http://www.mips.com.

[8] NEC electronics, Inc. http://ww.nec.com.sg/es.

[9] Dino Oliva, Rainer Buchty, Nevin Heintze. "AES and the cryptonite crypto processor". CASES 2003 Conference Proceedings, pp.198-209.