A High-Performance Platform-Based SoC for Information Security

Min Wu, Xiaoyang Zeng[+], Jun Han, Yongyi Wu, Yibo Fan
State Key Lab of ASIC and System, Fudan University, Shanghai 200433, China
[+] Email: xyzeng@fudan.edu.cn, Tel: 86-21-65104145.

Abstract-A platform-based SoC named as Firebird is presented in this paper, which is used for the applications of information security. Several design aspects, which includes the embedded 32-bit RISC CPU and AMBA controller, the reconfigurable and scalable public-key crypto-coprocessor, high-performance TRNG and several low-power schemes, make Firebird very efficient for the client-end applications of information security. Also the test results of this prototype chip indicate that Firebird can work with all these features efficiently, and has some obvious advantages over other designs in the literatures.

1. Introduction

Recently, Platform-based SoC (System-on-Chip) design has become an efficient solution to meet the continuously increasing requirements of Time-to-Market. In general, a SoC platform consists of embedded CPU and bone bus, DMA controller, memories, and some other assistant modules. With a SoC platform, diverse modules for special applications such as security IPs can be integrated easily.

In this paper, a platform-based SoC named as Firebird for information security is proposed. And it integrates several special sub-modules such as a public-key crypto-coprocessor, a full-customized TRNG (True Random Number Generator) and a USB engine in addition to the necessary modules for the SoC platform.

2. Architecture and merits description of Firebird

Figure 01 shows the hardware-level architecture of the SoC platform used for the design of Firebird, which consists of following several important modules: the embedded 32-bit RISC CPU and it AMBA bus that includes AHB (system bus) and APB (peripheral bus), the reconfigurable and scalable public-key crypto-coprocessor, TRNG (Truly Random Number Generator), USB engine and some other modules. Among these modules, CPU is the main controller for all information security protocols and algorithms; public-key crypto-coprocessor acts as the undertaker of all computations of complex arithmetic, which affects the overall performance of Firebird. And AMBA bus presents a flexible environment for modules' interface and communication.

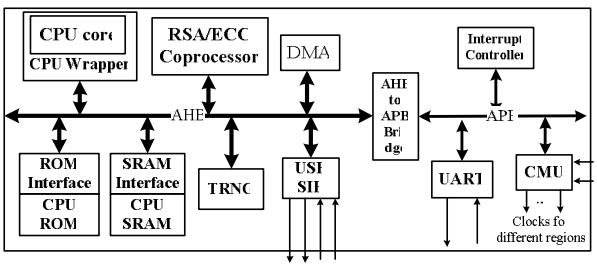

Fig. 01 Platform Architecture for Firebird

Comparing with other design in the literatures, Firebird has several merits such as the reconfigurable and scalable public-key crypto-coprocessor, high performance TRNG, and efficient low-power schemes, etc. And these merits make Firebird very suitable for the high-performance client-end applications of information security, especially for the fields of portable devices and wireless communications.

Fig.02 shows the architecture of crypto-coprocessor, the core part of Firebird. It can perform the complex arithmetic both of ECC and RSA, i.e., can carry out both point multiplication over elliptic curves and modular multiplication of big integers. The word-based scalable data-path is the most important part of the coprocessor, and it can perform several types of computation abovementioned with a word-based style using the same arithmetic unit without any other hardware modifications. The data-path can also perform two multiplications in finite filed operations in parallel, then speed up point multiplication of ECC, and save about half operating time. It can also be configured to implement up to 2048-bit modular multiplication.

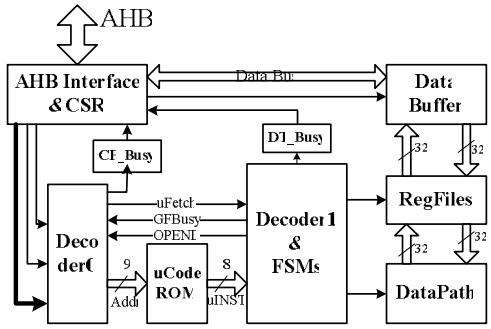

Fig.02 VLSI Architecture of RSA/ECC Coprocessor

TRNG module in Fig.01 shows another merit of Firebird and is mainly used for key generation and one of the countermeasure solutions for anti-attacks. In this design, a thermal noise based scheme is adopted. And the TRNG has passed the strict test with the international standards such as FIPS140-1 and NIST SP800-22. And the TRNG includes the advantages such as high-speed, low power and low cost.

Another important merit of Firebird lies in the low power schemes. A CMU (Clock Management Unit) is created for power saving for the applications such as portable devices and wireless communications. From the operation procedure of Firebird, it is determined that the three modules, e.g. public-key crypto-coprocessor, TRNG and DMA controller, will seldom work simultaneously. Hence a much higher power-efficiency will be achieved if their clocks are closed or waked-up by firmware-controlled CMU dynamically. One scheme of low power is shown in Fig.03. The embedded RISC CPU itself can also be clock-gated by firmware if there are no more tasks, and will be waked-up if any interrupt comes. In this way, the four main power consumers of Firebird are fully controlled by firmware to work or not, and a consequent overall power efficiency will be achieved.

The DMA controller in Firebird is used to improve the

0-7803-9451-8/06/$20.00 ©2006 IEEE.

throughput of bulks data transferring. In this paper, DMA Controller can be fully controlled by CPU. And it can be safely and easily clock-gated by firmware-controlled CMU.

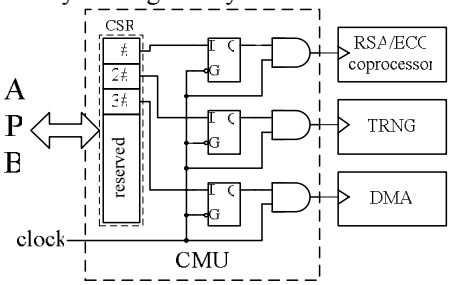

Fig.03 Scheme of Power Efficiency

In Firebird, several modules can share the internal buffers with CPU so as to avoid extra unnecessary operations of data copying. And this kind of architecture shown in Fig.04 is called sharing-memory and very efficient for USB engine and crypto-coprocessor, which must handle bulks of data.

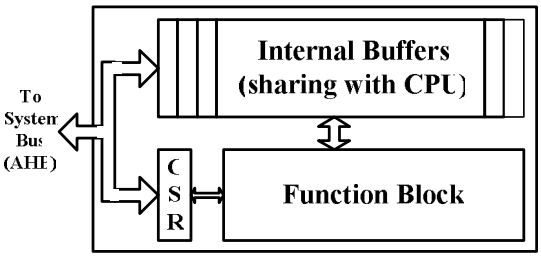

Fig. 04 Scheme for Sharing-Memory

3. Implementation and Test Results

The platform-based SoC, i.e. Firebird, is implemented with TSMC 0.25um CMOS technology and Fig.05 shows its die photo, and this prototype chip is pad-limited. The total die size is about 4.7885*4.3438mm2 (including pads). The test results indicate that: Firebird can work at 60MHz, and the main sub-modules such as crypto-coprocessor can work at 150MHz; the signature rate is about 20 times/sec (@50MHz) with RSA algorithm and 50 times/sec (@50MHz) with ECC algorithm. Fig.06 shows power dissipation of Firebird (@30MHz, 2.5V) during each working-stage, and there exists three kinds of power management level, which are the level of no power management (DPM0), no CPU clock-gated (DPM1) and CPU clock-gated (DPM2). It can be seen that the DPM (Dynamic Power Management) schemes can improve energy efficiency of Firebird and reduce the mean power from about 110mW to 70mW.

All above features are sufficient for the high-performance but low-cost-and-power client-end applications of information security such as the fields of portable devices and wireless communications. And they also have obvious advantages over other related implementations as Table 01 shows.

4. Conclusions

In this paper, a platform-based SoC for information security named as Firebird is presented. And it includes several merits such as reconfigurable and scalable public-key crypto-coprocessor, high-performance TRNG and several low-power schemes. Also the test results of this prototype chip of Firebird indicate that all these features can help Firebird to perform both RSA and ECC computations with reasonable power dissipation, acceptable low-lost but high performance, which are the key elements for client-end applications of information security.

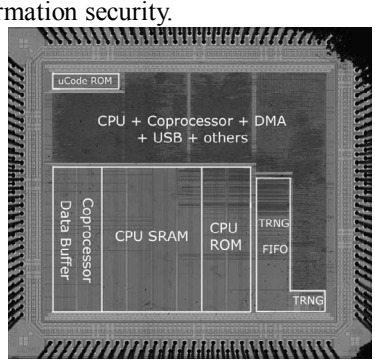

Fig. 05 Die Photo of Firebird

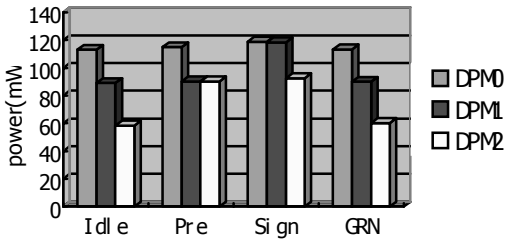

Fig.06 Power Dissipation Test and Comparison

Table 01 Some Comparison for Crypto-coprocessor

items / designs	Year	Power (mW)	Kilo gates	Tech (um)	Freq (MHz)	Baud rate (kbps)	Scalable
Ref. [6]	1989	500	-	2	25	8	N
Ref. [5]	1997	330	-	-	45	-	-
Ref. [4]	2003	-	40	0.35	220	69	Y
Ref. [3]	2002	-	77	0.6	300	72	N
Ref. [2]	2004	-	148	0.18	450	214	N
Proposed	2005	41.6	45	0.25	30	14	Y

(*) The work is sponsored by NNSF (National Natural Science Foundation)

Reference

[1]. W. Kim, S. Kim, et al., A Platform-Based SoC Design of a 32-Bit Smart Card, ETRI Journal, Vol.25, No.6, Dec. 2003, PP.510-516.

[2]. Q. Liu, F. Ma, D. Tong, et al., A regular Parallel RSA Processor, IEEE MWSCAS 2004, July 25-July 28,2004,Japan, PP. III467-III470.

[3]. J.H Hong, C.W Wu, Cellular array modular multiplier for the RSA Public-key cryptosystem based on modified Booth's algorithm. IEEE Trans. VLSI Systems, Nol.11, No.3, 2002, PP.474-484.

[4]. M-C. Sun, C-P. Su, et al., Design of a scalable RSA and ECC Crypto-processor, in Proc. ASP-DAC, Kitakyushu, Jan. 2003, PP. 495-498.

[5]. A. Satoh, Y. Kobayashi, et al., A high-speed small RSA encryption LSI with low power dissipation, in Proc. 1st Int. Information Security Workshop (ISW'97), Sept. 1997, Japan, PP.174-187.

[6]. A.Vandemeulebroecke, et al., A Single-chip 1024-bits RSA processor, in Proc. Advances in Cryptology (EUROCRYPT'89), Belgium, PP.219-236.