Design of a Dynamic Reconfigurable Microsystem Based on SIP

Hao Lv1,2, *, Shengbing Zhang1,a, Wei Han2,b, Yongqiang Liu2,c, Shuo Liu2,d, Lei Zhang1,2,e, Shiyu Wang1,f

1School of Computer Science, Northwestern Polytechnical University, Xi’an, China
2Xi’an Aeronautics Computing Technique Research Institute, Aviation Industry Corporation of China, Xi’an, China

*Corresponding author e-mail: lvhao20032003@qq.com, a zshb@nwpu.edu.cn,
bWH@qq.com, cYQ@qq.com, dSL2@qq.com, ezangleiactri@163.com,
fSyu@qq.com

Abstract. In recent years, with the development of microelectronics technology, microsystems based on SIP/SoC have been applied to drone and other avionics systems. It is practical to study the reconfigurable calculation of avionics microsystems facing the flexible use of the scene. Encryption/decryption data based on FPGA can adapt to different application environments and functional requirements, which is especially important for product protection. However, implementing multiple algorithms on the same chip leads to increased logic resource consumption, low resource utilization, and poor system flexibility. In view of the above problems, it is necessary to design a dynamic reconfigurable computing platform based on an aviation SIP micro-system chip with dynamic reconfigurable technology as the core (using Zynq SoC). The platform use on-chip ARM processor to control reconfiguration. The different encryption and decryption algorithm logics are configured into different logical partitions on the chip according to the requirement. The logic circuit is updated and the algorithm is reconstructed. Different encryption and decryption algorithms are implemented by using the HLS method. The verification results show that the design can complete the algorithm switching at a higher configuration speed while the other functions on the chip work normally. Under the premise of ensuring the stability of the system, the on-chip logic resource consumption is reduced, and the resource utilization and system flexibility are improved.

1. Introduction
In recent years, with the miniaturization and miniaturization of avionics and other avionics, microsystem technology has received more and more attention, and SIP and SOC are two important technical approaches for micro-system implementation. In the future, the miniaturization of avionics computers will adopt SIP integration technology to realize the integrated design of computer systems, greatly improve system storage capacity, bus bandwidth, processing performance, and reduce system volume and power consumption.
Heterogeneous multi-core processing platform integrates a variety of processors, which is different from the single core processor that can only execute instructions in sequence. Multi-core processor can perform different computing tasks concurrently, can work together to complete many complex functions, and meet the requirements of a variety of computing tasks. CPU + FPGA heterogeneous multiprocessor architecture combined with reconfigurable computing technology is a hot research direction [1].

In order to meet different application environments and security requirements, the encryption and decryption system needs to use different encryption and decryption algorithms to process the data. However, implementing multiple algorithms on the FPGA chip will further increase the logic resource consumption, and only use the same time. When an algorithm processes data, other algorithms still occupy a large amount of on-chip logic resources while not working. This reduces resource utilization. ALL the work processes need to be stopped when modifying and updating the application algorithm at the same time, and the entire system is shut down and maintained. This limits the flexibility of the system [2]. Therefore, it is of practical significance to study the reconfigurability of aeronautical computing microsystems.

For foreign trade computer products, it is particularly important to realize the encryption storage of its core algorithm software (control algorithm, guidance algorithm, etc.) for the security and protection of knowledge products. In this paper, different encryption algorithms are used to study the reconfigurability of specific microsystems.

A heterogeneous multi-core SIP chip with minimum computing system is designed and implemented by using the zynq-7000 SOC chip of Xilinx company facing the application requirements of avionics equipment, control system and computing platform, so as to flexibly adapt to different requirements in performance, volume and power consumption at the same time. The dynamic reconfigurable control platform is designed and implemented based on the dynamic reconfigurable technology. According to the design idea of time-division multiplexing for the on-chip logic resources, a variety of algorithm modules are stored in the memory, and specific logic areas are divided on the chip. The algorithm switching is completed by reconstructing the functional logic in the area. The computing task which can be carried out according to the computing needs is realized in the HLS mode. Taking AES and 3DES encryption and decryption algorithm as an example, it integrates with the control platform, tests and analyzes the performance.

2. Related Work

2.1. Reconfigurable computing technology

Professor Gerald Estrin put forward the concept of reconfigurable system in the 1960s[3]. More and more people began to study this technology with the continuous development of FPGA reconfigurable technology later. In some fields, they gradually made good achievements, such as neural network[4], gene group matching, space technology and other fields[5]. Reconfigurable computing is used to fill the gap of performance and flexibility between ASIC hardware computing and software computing. Generally, reconfigurable computing system adopts the form of highly coupling of reconfigurable hardware (mainly FPGA) and microprocessor. Reconfigurable computing hardware can achieve the performance close to ASIC, and maintain enough flexibility.

There are two kinds of reconfigurable technologies in FPGA: static reconfiguration and dynamic reconfiguration. Static refactoring refers to use the configuration file in the memory to logically configure the FPGA and change under the control of other components. FPGA can not do other work in the process of configuration. Dynamic reconfiguration means that in the process of configuration, the non reconfigurable area can work normally, only the local logic of FPGA needs to be reconfigured.

In terms of system performance and function, the University of Florida studied in the video algorithm of DCC using 2.3m bit stream. The research is based on the expandable characteristics of FPGA, using the The architecture of state local reconstruction is . In this paper, 80 different hardware architectures are realized by dynamic reconfiguration. The power consumption, clock cycle, and
reconfiguration cost of different architectures are analyzed and compared[6]. Brightam Yong University uses FPGA and DSP to research and implement a new dsp-rl structure, which can perform different calculations[7]. U.S.A Northwest University has designed a chimaera system to integrate dynamic reconfigurable functional units into dynamic .In the pipeline of scheduling. The University of California, Berkeley, has designed a system called GARP. In this system, MIPs microprocessor and FPGA are combined to study the ability to accelerate of reconfigurable unit in traditional processor[8].

2.2. AES and 3DES encryption and decryption algorithm

AES belongs to the block cipher algorithm. The block length is 128 bits, and the key length can be 128, 192 or 256 bits. The number of turns corresponding to AES is 10, 12 and 14 respectively[9]. The algorithm consists of four steps: sub bytes, shiftrows, MixColumns and addroundkey. The basic unit of each step is bytes. In the encryption process, first read in the plaintext and the initial key, add the two keys in turn, and expand the key based on the initial key; then, carry out byte replacement, row shift, column mixing with the state matrix in turn, and add the key in turn with the sub key of the corresponding number of rounds, and cycle 9 rounds; in the 10th round, skip the column mixing operation, and only carry out byte replacement, row shift and after round key addition, the state matrix is updated to ciphertext and output[10].

3DES algorithm is a block cipher algorithm based on DES algorithm. It is extended from single key to triple key. 3DES algorithm is formed by processing DES algorithm many times. The packet length and key length of DES algorithm are 64 bits. In the encryption process, the 64 bit plaintext is first replaced to get the 64 bit data in the scrambled position according to the rules. The data is divided into two parts of left and right 32 bits, which are represented by L0 and R0 respectively, and 16 rounds of iterations are started. In each iteration, the previous round RN-1 is directly taken as the LN of the current round, and the previous round RN-1 and the corresponding sub key of the next round are operated with F (R, K) function, and then the result is XOR with ln-1 to get RN. After the completion of the 16th round of iteration, a left-right exchange is carried out again, and L16 and R16 are spliced into 64 bits, and the ciphertext is output after the inverse initial replacement[11].

2.3. Zynq SOC

Zilinx's zynq-7000 SOC chip is suitable for constructing the SIP minimum system. Zynq SOC combines a dual core arm cortex-a9 processor and a field programmable gate array (FPGA) logic component[12]. This architecture realizes the industry standard Axi interface, and realizes the connection of high bandwidth and low delay between the two parts of the chip. According to the requirements, we can balance the hardware implementation and software implementation, so that they can work together, so that the design can meet the better index requirements.

3. Methodology

3.1. SIP microsystem

This avionics SIP micro system chip takes zynq SOC (z-7010) as the core, which includes processing system (PS) and programmable logic (PL). The PS end is dual core arm ® cortex ™ - A9, the maximum frequency is 667mhz, the PL end includes artix ™ - 7 FPGA, 28K logic cells and 17600luts. It can build a variety of peripheral device interfaces in PL through programmable logic. The PS end And PL end communicate with each other through industry standard Axi bus. Figure 1 shows the SIP chip. SIP also includes DDR3 memory with 128mbytes, SPI flash with 128Mbit, and interface driver. The internal composition of SIP chip is shown in Figure 2.
3.2. Reconfigurable platform design

The reconfigurable computing platform is composed of SIP chip, power supply, reset, clock and other peripheral circuits. The reconfiguration task of encryption algorithm includes zynq in SIP chip, ARM processor in PS terminal to complete the scheduling of dynamic encryption algorithm, and real-time replacement of encryption / decryption algorithm according to the instructions received by UART interface. Encryption and decryption algorithm is completed in FPGA in PL terminal. Figure 3 is a picture of the reconfigurable computing platform, which is inserted by the CPU board and the interface board; Figure 4 is the internal structure of the reconfigurable platform.

In the system design of FPGA, the area used for local reconfiguration is called dynamic area, and the design that does not need to be changed in the operation of the system is called static area. In the design of reconfigurable logic platform, the first step is to divide the logic module into static non reconfigurable logic part and dynamic reconfigurable logic part according to the function. The static non reconfigurable logic part refers to that when the system is in normal operation, the function and logic circuit structure are always the same, and the work tasks are executed according to the initial settings; while the dynamic reconfigurable logic part refers to that when the system is in normal
operation, multiple functions of the part will only execute one of them at a single time, and other functions are idle. In zynq, the reset control module, clock management module, data interconnection module, GPIO drive transmission module, UART communication module, reconfiguration data interface module and reconfiguration processing module always work according to the set function, which belongs to the static non reconfigurable logic part; and the multiple encryption and decryption algorithm modules that need to be switched can only be used one at a single time, so it belongs to the reconfigurable logic part.

Figure 4. Structure of reconfigurable computing platform

PRC provides management function for local dynamic reconfiguration. The main device can control PRC to locally configure the reconfiguration area during system operation through Axi Lite bus without affecting the static design of non reconfiguration area. When the dynamic reconfigurable configuration is triggered, the dynamic reconfigurable controller will obtain the reconfiguration file of the dynamic region from the memory through the Axi interface, and then reconfigure the dynamic reconfigurable region through the ICAP (internal configuration access port) interface. When reconfiguration occurs, the static area and dynamic area need to be isolated to ensure that the reconfigurable design of the dynamic area is in a safe state before removal, otherwise, after the completion of reconfiguration, various signals in the system appear disorder, resulting in the system can not operate normally. PR decoupler (partial reconfiguration decoupler) core can decouple the dynamic and static regions when the local reconfiguration occurs, ensuring the security state after the system reconfiguration. In this paper, the dynamic region uses the axi4 Lite mode to interact with the static region, so the partial reconfiguration decoupler is used to understand the coupling of the axi4 Lite mode, in which the control decoupling signal is generated by PRC.

Flash memory is responsible for storing logical configuration files of various encryption and decryption algorithms, which are configured to reconfigurable configuration partition on chip through dynamic reconfigurable control platform. The platform consists of two parts: the reconfigurable logic platform based on the PL part and the core controller based on the PS part. The control platform takes the reconfigurable logic platform as the carrier, designs the corresponding hardware logic to complete the functions of management system clock, control data communication and working state, and uses the core controller to control the dynamic writing of reconfigurable configuration file, dynamic scheduling of configuration tasks and access of internal data. When the task is running in real time, the corresponding logic can be configured into the specified logical resource area according to different functional requirements, and the logical unit and interconnection unit can be modified accordingly, so as to realize different structures and functions.

HLS (high level synthesis) is a kind of C specification that can be converted into RTL (register transformer level) tools can be integrated into FPGA finally. Users can write C specifications through C, C++, SystemC. Because of the advantages of FPGA in parallel structure, performance and power consumption. Using HLS to implement the hardware algorithm running on FPGA, in essence, is to synthesize the C language programming into RTL level design through HLS tools, and lay out the wiring on FPGA, and finally realize the hardware implementation of the computing task. The AES and
3DES encryption and decryption algorithms of the reconfigurable platform are completed by HLS tools.

4. Experimental design and analysis

This paper takes AES and 3DES as examples to integrate with the design, tests the reconstruction process of encryption and decryption algorithm, analyzes the relevant indicators of the reconstruction process, and verifies the correctness of using different encryption and decryption algorithms to process data.

The upper computer control software sends the corresponding reconstruction command to arm through UART port. ARM processor starts the reconstruction and displays the reconstruction return status in the interface. After the algorithm reconstruction, the key and plaintext / ciphertext data are transmitted to FPGA through the encryption and decryption data transmission port for encryption and decryption processing. The data returned after the encryption and decryption processing of AES and 3DES are compared with the data obtained by the standard encryption and decryption tool, and the data are the same, which proves that the encryption and decryption function can be carried out correctly after the reconstruction.

In this design, the file size of the overall encryption and decryption system is 4498144 bytes, and the reconstruction file size of the encryption and decryption algorithm function module is 785052 bytes. It can be seen that using dynamic reconfigurable technology to complete the encryption and decryption algorithm switching can effectively reduce the size of the configuration file, compared with modifying the algorithm function logic of the overall encryption and decryption system and downloading it to the FPGA chip again. Under the condition of continuous and stable operation, the function of encryption and decryption algorithm is modified to improve the flexibility of the system. The type of encryption and decryption algorithm in external memory can be modified flexibly according to the functional requirements. The system has scalability and can adapt to different working environment requirements. After the completion of the function test, the key control signal and the reconstruction status return signal are connected to the logic analyzer through the extended pin of FPGA. The configuration time of the reconstruction process of the encryption and decryption algorithm is measured to be 46.19 ms, and the configuration speed is calculated to be 16996.14 bytes/ms, which shows that the dynamic reconfigurable control platform designed in this paper can control the configuration file of the encryption and decryption algorithm module to finish at a higher configuration speed. The algorithm has good control performance.

Then the encryption and decryption time of 3DES algorithm in pure software mode and FPGA acceleration mode are tested and compared. The test uses SIP based reconfigurable computing platform, and the linaro 14.04 operating system (for arm's lightweight Linux system) which runs on zynq dual core arm (coretx-a9).

Mode 1: read out data from flash memory by ARM processor, and complete data encryption and decryption by pure software in DDR3 memory;

Mode 2: the arm processor reads out the data from flash memory and writes them to FIFO in the PL FPGA in turn. The PL FPGA completes the encryption and decryption process and places the final data in DDR3 memory.

Test data is shown in Table 1, FPGA acceleration can significantly shorten the time of encryption and decryption obviously, and the acceleration ratio is 1.49.

| Data(Mb) | ARM(double Coretx A9) (s) | ARM(double Coretx A9)+FPGA (s) |
|---------|--------------------------|-------------------------------|
| 3       | 0.1393091                | 0.09704                       |
| 12      | 0.590645                 | 0.379954                      |
| 24      | 1.157414                 | 0.768384                      |
| 48      | 2.31054                  | 1.542494                      |

Table 1. Comparison of 3DES algorithm time test
5. Conclusion
This paper introduces the design and implementation process of a reconfigurable micro system based on SIP (including zynq, memory, etc.), explains and introduces its dynamic reconfigurable principle and design with AES and 3DES encryption and decryption algorithm. The time of reconfigurable configuration is compared and tested based on the reconfigurable computing platform. The time of 3DES algorithm encryption and decryption is compared under the combination of pure software and hardware. It meets the multi-objective constraints of the volume, power consumption and performance of Microelectronics System, reduces the consumption of resources on chip, ensures that the encryption and decryption system can complete the switching of encryption and decryption algorithm types at a high configuration speed in a stable working state, improves the utilization rate of resources on chip, and makes the system more flexible. The reconfigurable platform has universality and can be used as reference for the design of avionics systems. In particular, it has important reference value for the research on the reconstruction and acceleration of navigation control algorithms in different flight phases of UAV systems. The platform will be further tested and studied in the future with different navigation control algorithms.

References
[1] RUI Cao. (0). Design and Implementation of Wearable Dynamic Reconfigurable Platform Based on Zynq (Doctoral dissertation).
[2] CHEN Xiang-ju,WANG Zhu,YAO Yan,TONG Xiao-Jun,LUO Qing-hua. (2019). Reconfigurable design of multiple encryption and decryption algorithms based on FPGA. COMPUTER ENGINEERING AND DESIGN, 40 (03), 56-60+68.
[3] Estrin G. Organization of Computer Systems-the Fixed Plus Variable Structure Computer[C]// afips. IEEE Computer Society, 1960:33-40.
[4] Eldredge J G, Hutchings B L. Density enhancement of a neural network using FPGAs and runtime reconfiguration [C]// FPGAs for Custom Computing Machines, 1994. Proceedings. IEEE Workshop on. IEEE, 2002:180-188.
[5] Hancher M D, Hornby G S. 2nd IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT'06) [J]. 2006.
[6] Huang J, Parris M, Lee J, et al. Scalable FPGA-based architecture for DCT computation using dynamic partial reconfiguration [J]. Acm Transactions on Embedded Computing Systems, 2009, 9 (1): 1-18.
[7] Kretzschmar U, Gomez-Cornejo J, Astarloa A, et al. Synchronization of faulty processors in coarse-grained TMR protected partially reconfigurable FPGA designs [J]. Reliability Engineering & System Safety, 2016, 151:1-9.
[8] Hauser J R, Wawrzynek J. Garp: a MIPS processor with a reconfigurable coprocessor [C]// IEEE Workshop on Fpgas for Custom Computing Machines, Apr. 1997: 12-21.
[9] Zhu, Y., Zhang, H., & Bao, Y. (2014). Study of the AES Realization Method on the Reconfigurable Hardware. International Conference on Computer Sciences & Applications.
[10] Wankhade, S., & Mahajan, R. (2014). Dynamic partial reconfiguration implementation of aes algorithm. International Journal of Computer Applications, 97 (3), 15-18.
[11] Qian, W., Wu, L., Zhang, X., Li, X., & Guo, J. (2013). Efficient Countermeasures against Fault Attacks for 3DES Crypto Engine in Bank IC Card. Ninth International Conference on Computational Intelligence & Security.
[12] Crockett, L. H., Elliot, R. A., Enderwitz, M. A., & Stewart, R. W. (2014). The Zynq Book: Embedded Processing with the Arm Cortex-A9 on the Xilinx Zynq-7000 All Programmable Soc.