International Journal of Engineering & Technology, 7 (4.36) (2018) 80-83

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Increasing the Efficiency of Microprocessors in an Access Control Systems

S.G. Magomedov.

MIREA - Russian Technological University,Russia

Abstract

This paper is devoted to the problem of improving the performance of microprocessors used in access control systems. The requirements are described, and a set of commands is proposed, that are necessary for efficient design of microprocessors working on the basis of the residue number system for the purpose of monitoring and access control. The proposed approach is aimed at improving the efficiency of microprocessor operation as part of the access control system.

Keywords: *function, microprocessor, commands, system, modular.*

1. Introduction

The general scheme of the device and the functioning of microprocessors (MP), presented in1, is proposed to be modified taking into account the possibilities of using the MP as one of the key elements of the access control system(ACS).

As it was stated in2, the ACS system is one of the key components of the information security system. Therefore, the requirements for all elements that are part of the system of ACS, including the MP, should be more elevated. In this regard, the composition of functions implemented in the said MP is called its microprocessor for access control and management (MP-ACS). Thus, when analyzing and forming the composition of functions within the MP-ACS, it is necessary to provide for a number of new opportunities and functions not implemented in the model MP, it is also advisable that the MP-ACS be designed taking into account the following requirements that are aimed at increasing the efficiency of their work in the composition of the ACS.

I. Data processing in closed format. The goal of data processing in closed format is to minimize the volume of conversions from the closed data storage format, which is intended to be used when storing data in RAM, to the open format,in case an open data processing mode is used by the processor, or another closed format. In the work of1 the advantages of using the calculation and transformation in the residue number system as a closed processing mode have been described.

II. The possibility of parallel processing of data. If there is a possibility of parallel data processing, it can be used to provide a higher level of encryption key strength and associated processes for processing private data. It is also applicable if several access requirements have to be completed simultaneously. It is also worth mentioning another important advantage of using the residue number system (RNS) which is proposed above as the main basis for designing microprocessors for access control: the execution of arithmetic operations in the RNS is much easier to parallelize than in other encryption systems, since calculations and transformations performed on different prime numbers included in the key basis can be executed independently, as described by8,11. This quality of the RNS opens up opportunities for active use of GPUs, which provide performance in computational operations at least an order of magnitude higher than that of existing microprocessors, which can increase the stability of the encryption system by significantly increasing the number and length of prime numbers in the RNS base.

III. Microprocessor for access control must be a specialized processor. That is, it has to have its own specific set of commands, which should be the most adequate to the scope of its use, namely the access control system. Therefore, it is necessary to select the minimum required set of commands. Below we propose a possible procedure for the development of the concept of the described microprocessor for access control and a set of commands built on the basis of the implementation of this procedure.

2. Research Method

For forming a set of commands (elementary operations) we will rely on the set of basic functions of microprocessors for access control listed by2.

1) Executing the operations given in the command code and related to the data conversion. First of all, this function includes the commands used to check various access attributes: passwords, access keys, authentication tokens, biometric data, and so on. Such commands are currently actively using various operations related to cryptographic transformations, in particular, arithmetic operations, especially exponentiation operations, and matrix operations. Moreover, all these operations, as follows from the above discussion of the problem, must be carried out in modular arithmetic, as described by7. This class includes all arithmetic and logical commands. Further we list the groups of these commands in accordance with their standard classification - the basic system of microprocessor instructions (grouped by functional purpose):

1. Arithmetic commands.
2. Logical commands.
3. Shift commands.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In addition there are also extension commands, described in3: X87 - commands of the mathematical coprocessor (processing real numbers); MMX - commands for encoding / decoding streaming audio / video data, SSE, SE2, SSE3, SSE4 - commands for performing operations with scalar and packed data types, for stream processing of integer data.

Also in addition to the listed groups of commands it is necessary to add the commands associated with performing a series of operations in modular arithmetic:

4. Exponentiation commands in modular arithmetic.

5. Matrix operations in modular arithmetic.

If the data is closed and the data processing procedure does not involve working with closed data, then the data should first be opened, that is, transferred from the closed format to the open one. If the processing procedure allows working with closed data, then the data access keys should be pre-installed, which are then used during processing. Thus, two more functions can be singled out, formally analogous to the standard ones, but the actual content of which is much more complicated.

2) The function of deciphering the incoming command (selecting a command from the data entry bus and decrypting it). These operations are designed to decode the command received from the bus, then select individual components of the command in accordance with its specified pattern for the subsequent use of these components during data processing. It will be mentioned further that the process of data exchange between different microcontrollers can be closed on the basis of procedures that do not use encryption methods, but rely on RNS, as shown by4. In this case, it becomes necessary to open (decrypt) this data. In the case of access control systems, the most important groups of commands are:

1. Input-output commands.

2. Commands for working with the stack.

3. Type conversion commands.

Additionally, a following group of commands is added:

4. Commands for decrypting data received from the control bus.

Stack commands are required in cases where part of the data queued for processing is placed on the stack. Type conversion commands are necessary to perform changes of data structures in order to more efficiently process them, for example, to interpret integer data of a standard size as large numbers or small.

3) Data decryption function, that is, the selection of addresses and data contained in the command, the selection of data and keys (the formation of the key combination) with which they were closed, and the subsequent decryption of data based on these keys. In different situations, as described by4,9,10 individual commands from the following groups may be required5:

1. Stack commands – required if it is necessary to select a part of the data from the stack.

2. Arithmetic commands in modular arithmetic – required in the implementation of algorithms for decryption and key generation in RNS8,11.

3. Type conversion commands – required if it is necessary to convert data types in order to improve the efficiency of their processing.

4. Processor synchronization commands – required to use parallel computing when working with keys in RNS.

It is also advisable to introduce the following additional groups of commands (they were already mentioned above):

- for decrypting the received data:

5. Exponentiation commands in modular arithmetic.

6. Matrix operations in modular arithmetic.

- for selecting data and addresses:

7. Logical commands.

Similar functions are implemented when data is transferred from microprocessors for access control.

4) The function of forming the command address for closing the data contained in this command (if any) and placing the command in the address memory bus (via the data bus). The same command groups as in the previous function are used, as well as the data transfer commands.

5) The function of managing encryption keys. The main operations are related to the control of encryption keys: creation, updating on expiration or loss of keys, placing data in databases or archiving data, etc. Therefore, the following groups of commands are necessary.

1. Data transfer commands – required to select data according to encryption keys and to transfer keys to recipients.

2. Commands for setting a single bit – required to block possible attempts of external interference in the process of obtaining key data and transferring keys.

3. Stack commands – may be required when working with different encryption keys.

4. Arithmetic commands – required for updating, restoring and creating encryption keys in the RNS.

5. Logical commands – required for analyzing various situations associated with the updating and recovery of encryption keys.

6. Flag control commands.

7. Interrupt commands – may be required when working with encryption keys to block possible attempts of external interference.

8. Control transfer commands – required when using different procedures related to the creation and updating of keys.

9. Processor synchronization commands – required for the parallel usage of multiple cores (processors) in the process of creating RNS keys and data encryption.

6) The function of implementing a number of procedures of the certifying center, as described by [6], which are carried out during transfer of data from one component of the microprocessor to another. The most important groups of commands for this function are the following:

1. Data transfer commands – required for the transfer of closed data to different components which interact with the microprocessors for access control or are being controlled by the microprocessor.

2. Commands for setting a single bit – may be required for creating secure transmission channels or restricting access of other components to the system when interacting with a particular system element.

3. Stack commands – can be used to control the process of transferring or exchanging encryption keys.

4. Flag control commands – similar to group 2.

5. Interrupt commands – required for emergency intervention in the processing of data, if necessary.

6. Processor synchronization commands – required to use parallel data processing involving different components of the system.

Additionally, another group of commands is necessary, which is related to verifying the authentication data coming from different components:

7. Comparison and verification of authentication tokens in accordance with a given pattern of the token structure.

7) The function of the systematic generation of state signals, as well as control and timing signals, and the transmission of these signals to the input-output control and memory management devices. It should be noted that this function is necessary for the operational control of the state of the microprocessor for access control and its individual elements. The main groups of required commands are the following:

1. Commands for setting a single bit – required to block the possibility of external interference in the process of collecting system state data, including the state of the microprocessor for access control.

2. Type conversion commands – required for generating a status string.

3. Flag control commands – similar to group 1.

4. Bitwise scan commands – required for selective collection of data from a given data aggregate.

5. String commands – required for creating a status string and working with it.

It is also advisable to introduce a function that extends the capabilities of string commands for the purpose of forming strings from heterogeneous data:
6. Commands for processing strings composed of various types of data.
8) The function of saving the results of an operation in memory or internal registers. These results are often part of the chain in the data processing procedure. Required groups of commands include the following:
1. Data transfer commands – required to move data to the target registers or addresses in internal or external memory.
2. Commands for setting a single bit – required for isolating and controlling the location of the data.
3. Flag control commands – similar to group 2.
4. Processor synchronization commands – required for synchronization of data storage processes with other processes related to the processing of the data.
9) The function of receiving and responding to control signals coming from the outside, as well as to high-priority signals, in particular, related to interrupts. This function is one of the most important functions in case various non-standard and emergency situations occur10.
1. Commands for setting a single bit – required to isolate different components of the system in order to avoid undesired interaction of processes or interference, especially when processing non-standard situations.
2. Stack commands – required for simultaneous processing of several control signals.
3. Flag control commands – similar to groups 1 and 2.
4. Interrupt commands – used in the process of handling non-standard situations.
5. Control transfer commands – required to activate the procedures associated with different types of violations in the system and with emergency situations.
6. Processor synchronization commands –required to ensure the consistent operation of different processes associated with processing a non-standard situation.

3. Results and Analysis

The results of the analysis can be presented in the form of the following table.

Table 1. The relevance of different command groups to various functions of microprocessors for access control

#	Name of command group	Function numbers of microprocessors for access control									Total functions
		1	2	3	4	5	6	7	8	9	
1	Arithmetic commands	+	-	+	+	+	-	-	-	-	4
2	Logical commands	+	-	+	+	+	-	-	-	-	4
3	Shift commands	+	-	-	-	-	-	-	-	-	1
4	Exponentiation commands in modular arithmetic	+	-	+	+	-	-	-	-	-	3
5	Matrix operations in modular arithmetic	+	-	-	-	-	-	-	-	-	1
6	Input / output commands	-	+	-	-	-	-	-	-	-	1
7	Stack commands	-	+	+	+	+	+	-	-	+	5
8	Type conversion commands	-	+	-	-	-	-	+	-	-	2
9	Commands for decrypting data received from the control bus	-	+	-	-	-	-	-	-	-	1
10	Synchronization commands	-	-	+	+	+	+	-	+	+	6
11	Data transfer commands	-	-	-	+	+	+	-	+	-	4
12	Commands for setting a single bit	-	-	-	-	+	+	+	+	+	5
13	Flag control commands	-	-	-	-	+	+	+	+	+	5
14	Interrupt commands	-	-	-	-	+	+	-	-	+	3
15	Control transfer commands	-	-	-	-	+	-	-	-	+	2
16	Commands for comparing and verifying authentication tokens	-	-	-	-	-	+	-	-	-	1
17	Bitwise scan commands	-	-	-	-	-	-	+	-	-	1
18	String commands	-	-	-	-	-	-	+	-	-	1
19	Commands for processing strings composed of various types of data	-	-	-	-	-	-	+	-	-	1

In the list of the basic system of microprocessor commands in the table there are no correction commands for binary-decimal numbers, which are mainly required for input / output of large amounts of numerical data, which is typical for commercial activities and economy, but not for access control.
It can be concluded from the table that the following command groups are the most commonly required: synchronization commands (required in 6 functions), stack commands, commands for setting a single bit and flag control commands (required in 5 functions), which are important in the access control process, arithmetic and logical commands (required in 4 functions), which are associated with computational operations carried out during access attributes checking and closing / decrypting of data. The highly specialized command groups turned out to be in lower demand.

4. Conclusion

However, the numerical estimates given above do not take into account a number of important applied characteristics of the process of microprocessor operation in the access control system. These applied characteristics will be the subject of further study in the following work.
1) the importance of this class of functions for the ACS system. This characteristic is directly related to the subject area for which specialized MP - areas of control and access delimitation in security systems are created; also covers such properties of the system as the requirements for the degree of stability of the systems of encryption / decryption of data, the scale of the use of MP.
2) frequency of use of this function. This characteristic is also related to specific conditions for the use of the MP-ACS being created.
3) the complexity of the implementation of each function, which largely determines the time of implementation of this function, the costs of creating MP-ACS, their speed, complexity of operation, the reliability of the MP-ACS, as well as the number of specific functions included in each class.

References

[1] Magomedov Sh. Organization of secured data transfer in computers using sign-value notation//ITM Web of Conferences. 2017. T. 10 DOI: 10.1051/itmconf/20171004004
[2] Magomedov Sh.G. Classification of access boundaries and associated factors of influence in the access control system / Bulletin of the Astrakhan State Technical University. Series: Management, Computer Science and Informatics. 2018. № 1. P. 62-70. DOI: 10.24143 / 2072-9502-2018-1-62-70
[3] https://en.wikipedia.org/wiki/Mathematical_Supcessor

[4] Osinin I.P. Modular-Logarithmic Coprocessor for Mass Arithmetic Computations / Bulletin of South-Ural State University. Series: Computational Mathematics and Informatics. 2017. T. 6. № 2. P. 22-36.
[5] The basic system of commands of the microprocessor // https://prog-cpp.ru/asm-command/#mov
[6] Magomedov Sh.G., Morozova T.Yu., Akimov D.A. Ensuring the security of data transmission in computer networks based on the use of residual class systems / Information Security Problems. Computer systems. 2016. № 3. P. 43-47.
[7] Chervyakov N.I. Modular structure of the parallel computing systems neuroprocessor. 288 p. Moscow, Publishing Fizmatlit.
[8] Omondi A. Residue Number System: Theory and Implementation. London: Imperial College Press, 2007. 312 p.
[9] Kogelman LG, Artozey E.A. Model of information security system. access control system / Modern information technologies. 2016. No. 23. P. 94-98.
[10] Kazantsev IS Methods of identification and authentication of the operator in modern systems for monitoring and controlling access to information / Current trends in the development of science and technology. 2016. № 5-3. Pp. 63-66.
[11] Omondi A., Premkumar B. Advances in Computer Science and Engineering: Texts. Vol. 2 Residue number system. Theory and Implementation. London: Imperial College Press, 2007. 296 p