SOFTWARE-HARDWARE FACILITIES FOR CRYPTOSYSTEMS BASED ON POLYNOMIAL RNS

M. Kalimoldayev, S. Tynymbayev, M. Magzom

The Institute of Information and Computational Technologies
050010, Almaty, Republic of Kazakhstan

This paperis dedicated to the development of software-hardware facilities for cryptosystems based on polynomial residue number system.

Today, there is a significant increase in the transfer and processing of personal data from different sources, and this huge amount of data is stored in various information systems and environments. There are many security threats to sensitive data that are processed and stored on such systems.

One of the most reliable ways to solve data protection problems in computer systems and networks is data encryption. With the development of communication networks and embed systems, there is a growing need to create efficient hardware solutions for performing encryption.

The most of the known conventional software-hardware cryptosystems are implemented using positional number system. The main difficulty with performance occurs during work with large data blocks (for instance, with long encryption keys) in cryptographic transformations.

As a result of searching for ways to increase the productivity of electronic computers, methods of detecting and correcting errors, and building highly reliable computer systems, in the middle of the 20th century research has begun in the field of non-positional notation systems.

In this article we discuss some aspect of software and hardware implementation of the encryption scheme based on polynomial residue number system (RNS), which is a system of data representation in computational arithmetic. In RNS, a multi-digit integer in the positional number system is represented as a sequence of several small-digit positional numbers. These numbers are the residues (deductions) from dividing the original number by the bases of the RNS, which are mutually prime numbers.

RNS is the one of the known methods for optimizing computations in existing cryptographic algorithms. It is a nonpositional number system, which is also known as modular arithmetic. In particular, the usage of systems of residual classes allows to increase the speed of operations due to lack of carry bit transfer during addition and splitting a large block of input data into smaller sub-blocks and their parallel processing.

Absence of digits transfer in operations of addition and multiplication and no error propagation is the main advantage that allows to effectively using residue number system in some areas of computer technology. All elements of the vector in nonpositional notations are equivalent unlike the positional notations and error in one of them leads only to a reduction in the dynamic range. This fact allows designing devices with increased fault tolerance and error correction.

A work is being done to develop and implement a software-hardware system for preliminary calculation of the parameters of the non-position number system. In this implementation, the main time-consuming operation — division of a polynomial modulo an irreducible polynomial — is performed hardware-wise on a multiplication device, the scheme of which was presented in authors' previous works.

The polynomial data for multiplication is prepared on the MicroBlaze software microprocessor, and then this data is transferred to the multiplier device to be multiplied by a modulo of an irreducible polynomial.

Currently a research project on the hardware implementation of the considered cryptosystem is in progress. As was shown above, the main advantages of using the nonpositional number system are the absence of transfer of bits in the operations of addition and multiplication, and, consequently, the possibility of parallel execution of operations on each of the bases of the system, which significantly speeds up the calculation process.

The developed design is to be implemented in HDL Verilog language and synthesized using the Xilinx Artix-7 FPGA.

The ongoing research is aimed for the development of algorithms for multiplying polynomials modulo irreducible polynomials, the synthesis and implementation of various digital multiplier circuits on their basis for the purpose of the software-hardware implementation of symmetric cryptosystems based on the nonpositional number system. The developed modular multiplier is planned to be used as a main calculation unit during hardware implementation of the proposed encryption systems built on NPNS so that calculation in the residue number system can be performed more efficiently in hardware.

In the developed multiplier, the product of polynomials is calculated by summing the rows of matrices of the partial product using multilevel tree of adders. After that a modular reduction by irreducible polynomial is performed.

The application of the non-positional number system allows accelerating slow calculations in asymmetric encryption algorithms and increasing their reliability as well.

Key words: residue number system, block cipher, nonpositional polynomial notation, FPGA programming.

References

1. Gura N. „Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs“ Proc. 6th Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES 04) LNCS 3156. Springer, 2004. P. 119–132.

2. Kumar S. Elliptic Curve Cryptography for Constrained Devices, doctoral dissertation, Electrical Engineering and Information Sciences. Bochum: Germany; Ruhr University, 2006.

3. Omondi, B. Premkumar, Residue Number Systems: Theory and Implementation, 2007.

4. Biyashev R., Nyssanbayeva S. Algorithm for Creation a Digital Signature with Error Detection and Correction // Cybernetics and Systems Analysis. 2012. V. 48. № 4. P. 489–497.

5. Kalimoldayev M., Nyssanbayeva S., Magzom M. Model of nonconventional encryption algorithm based on nested Feistel network // Open Engineering. 2016. № 6. P. 225–227.

6. Biyashev R., Kalimoldayev M., Nyssanbayeva S., Magzom M. Development of an encryption algorithm based on nonpositional polynomial notations // Proceedings of the International Conference on Advanced Materials Science and Environmental Engineering (AMSEE 2016). Chiang Mai, Thailand, June 26–27, 2016. P. 243–245.

7. Biyashev R., Nyssanbayeva S., Begimbayeva Ye., Magzom M. Building modified modular cryptographic systems // International Journal of Applied Mathematics and Informatics. 2015. V. 9. P. 103–109.

8. Tynymbayev S., Kapalova N., Magzom M. Development and implementation of a hardware multiplier in the non-position numeral system (in Russian) // Proceedings of IICT conference „Modern problems of computer science and computer technologies“. Almaty, 2017. P. 263–270.

9. Arty A7: Artix-7 FPGA Development Board for Makers and Hobbyists. [El. Res.]: https://store.digilentinc.com/arty-a7-artix-7-fpga-development-board-for-makers-and-hobbyists/ (may 2018).

10. Acosta A., Addabbo T., Tena-Sбnchez E. Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview // Int. J. Circ. Theor. Appl. 2017. № 45. P. 145–169.

11. Rooju Chokshi, Krzysztof S. Berezowski, Aviral Shrivastava, Stanisiaw J. Piestrak. Exploiting Residue Number System for Power-Efficient Digital Signal Processing in Embedded Processors // Proceedings of the CASES '09, Grenoble, France, P. 19–28.

12. Schinianakis D., Stouraitis T. Residue Number Systems in Cryptography: Design, Challenges, Robustness // Secure System Design and Trustable Computing. Springer, 2016.

13. Sousa L., Antro S., Martins P. Combining residue arithmetic to design efficient cryptographic circuits and systems // IEEE Circuits and Systems Magazine, 2016.

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ДЛЯ КРИПТОСИСТЕМЫ НА ОСНОВЕ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

М. Н. Калимолдаев, С. Т. Тынымбаев, М. М. Магзом

Институт информационных и вычислительных технологий КН МОН РК
050010, Алма-Ата, Казахстан

УДК 004.056.5

В данной статье рассматриваются некоторые аспекты программно-аппаратной реализации криптографической системы на базе непозиционной системы счисления. Описываются работы по разработке и реализации аппаратного умножителя полиномов по модулю неприводимого полинома с коэффициентами над GF (2) для непозиционной криптосистемы на базе ПЛИС. Рассматриваются некоторые вопросы создания программы предварительного расчета параметров непозиционной системы счисления с применением веб-технологий.

Ключевые слова: система остаточных классов, блочный шифр, непозиционная полиномиальная системы счислений, ПЛИС.

Today, there is a significant increase in the transfer and processing of personal data from different sources, and this huge amount of data is stored in various information systems and environments. There are many security threats to sensitive data that are processed and stored on such systems.

According to the steady growth in the number of users and devices in communication networks, issues of ensuring information security of data transmitted are particularly relevant. Cryptographic means of information protection can be used to solve the problems of confidentiality and authentication.

The main tasks of cryptographic protection of information in information systems are: data encryption to ensure confidentiality during storage and transmission over the network be-tween communication sites; the usage of hash functions to control the integrity of data; usage of message authentication codes and electronic digital signatures for message authentication.

One of the most reliable ways to solve data protection problems in computer systems and networks is data encryption. With the development of communication networks and embed systems, there is a growing need to create efficient hardware solutions for performing encryption.

Today, several efficient and reliable encryption algorithms and schemes are known. However, most of the known software-hardware cryptosystems are implemented in positional number system [1, 2]. The main difficulty with performance occurs during work with large data blocks (for instance, with long encryption keys) in cryptographic transformations.

When performing arithmetic operations on large digit numbers represented in the positional system, it becomes necessary to consider inter-digit carry propagation, which significantly slows down the calculation speed and complicates the structure of the device. The search for new ways to improve the performance of computing devices led researchers to the objective conclusion that in this direction of the positional number system all possibilities are exhausted.

In order to significantly improve the performance of computing devices, it is necessary to use the numbering systems devoid of such drawbacks.

As a result of searching for ways to increase the productivity of electronic computers, methods of detecting and correcting errors, and building highly reliable computer systems, in the middle of the 20th century research has begun in the field of non-positional notation systems.

In this article we discuss some aspect of software and hardware implementation of the encryption scheme based on polynomial residue number system (RNS).

1. Residue number system. In the traditional positional number system, the value of each numeric character (digit) in the number designation depends on its position, or the digit of the recording. The name of the positional number systems is determined by the bases of these systems. The basis of the sys-tem can be any number.

In addition to positional number systems, there are also non-positional number systems in which the notation of numbers is based on other principles. An example of such systems is known Roman numerals, which are written in the form of symbols meaning the value of the digit.

Another example of a non-positional system is residue number system (RNS) [3] , which is a system of data representation in computational arithmetic. In RNS, a multi-digit integer in the positional number system is represented as a sequence of several small-digit positional numbers. These numbers are the residues (deductions) from dividing the original number by the bases of the RNS, which are mutually prime numbers.

RNS is the one of the known methods for optimizing computations in existing cryptographic algorithms. It is a nonpositional number system, which is also known as modular arithmetic. In particular, the usage of systems of residual classes allows to increase the speed of operations due to lack of carry bit transfer during addition and splitting a large block of input data into smaller sub-blocks and their parallel processing.

Absence of digits transfer in operations of addition and multiplication and no error propagation is the main advantage that allows to effectively using residue number system in some areas of computer technology. All elements of the vector in nonpositional notations are equivalent unlike the positional notations and error in one of them leads only to a reduction in the dynamic range. This fact allows designing devices with increased fault tolerance and error correction [4].

In this paper we discuss implementation aspect of the symmetric encryption algorithm based on polynomial RNS (nonpositional polynomial number system, NPNS), described in [5–7].

2. Implementation of the softwarefor preliminary calculation RNS parameters. Preliminary calculation of the parameters of NPNSis performed in a software package, based on the library developed earlier for working with polynomials with coefficients over GF (2). The library implements following operations:

— addition;
— subtraction;
— multiplication;
— division.

The division operation is used in modular reduction by irreducible polynomial, an example of which is illustrated in Figure 1. There is a polynomial x6+x5+x2+1 is divided by x4+x3+x+1, forming a reminder x3+1. The library uses a binary representation of polynomials with coefficients GF (2).

```
 1100101
--------- = 100, r = 1001
  11011
```

Fig. 1. Division operation by irreducible polynomial

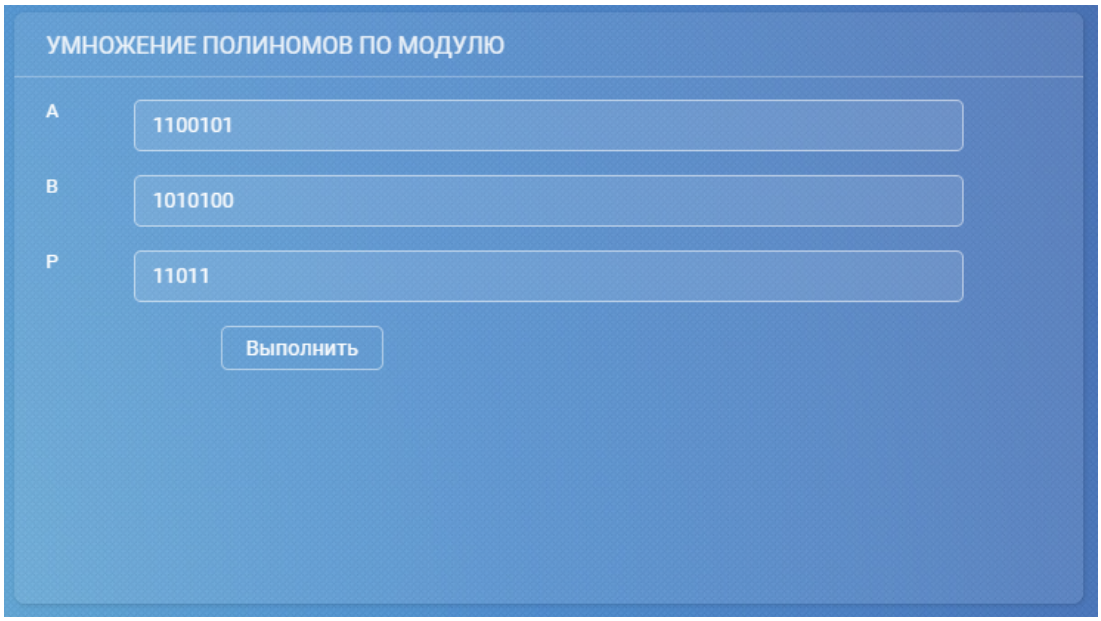


Fig. 2. Calculator form for modular multiplication

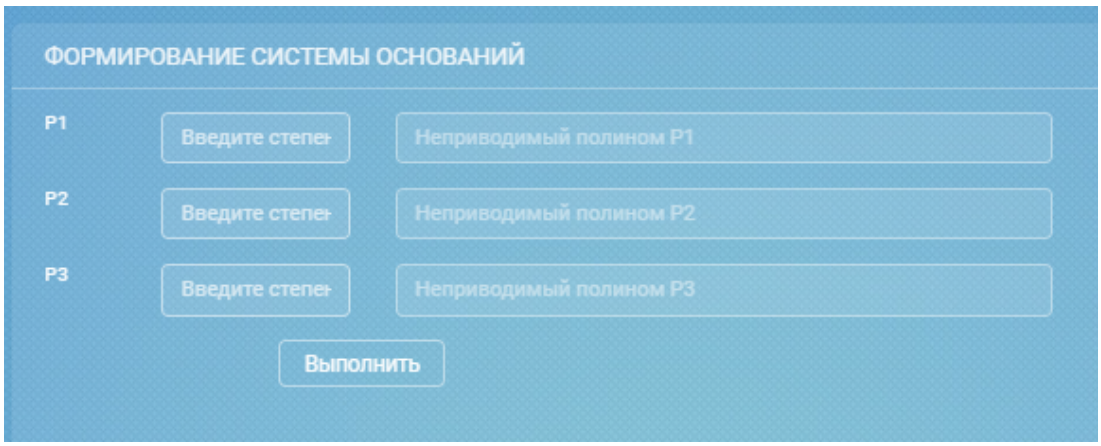


Fig. 3. Input form for the parameters of RNS

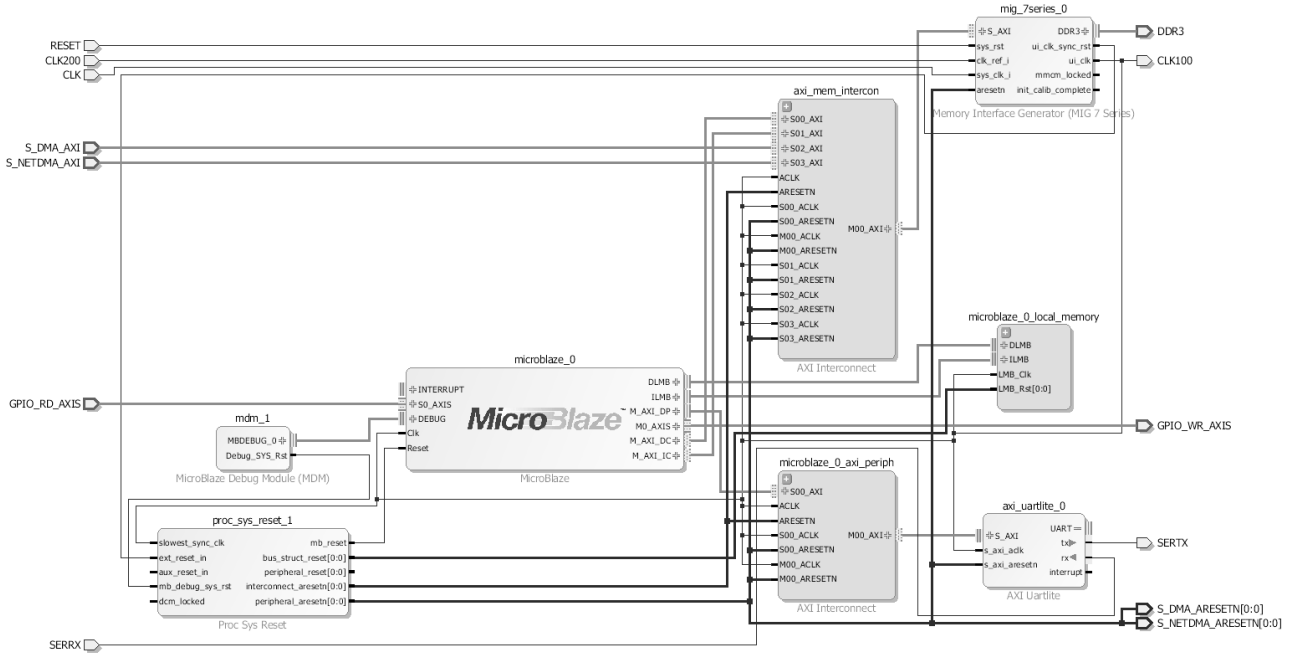


Fig. 4. MicroBlazemicroprocessor in Vivado development environment

To provide access to the means of calculation, a web interface was developed on the basis of the Spring framework.

The Spring MVC framework implements the Model-View-Controller pattern architecture using loosely coupled ready-made components. The MVC pattern separates the aspects of the application (input logic, business logic and UI logic) while providing a free link between them.

Model encapsulates application data, as a whole they consist of mathematical- computer models for computations in NPNS.

View is responsible for displaying the data of the Model, usually generating HTML, which is visible in a browser.

Controller processes user's request creates the corresponding Model and passes it to the View.

After the final selection of the components and their implementation, the architecture of the web application with the directories ready for further filling was obtained. Fragments for interaction with the visual part, CSS graphic styles, standard HTML pages and JavaScript functionality are located in the „resources“, and the models for calculation and control logic, respectively, are placed in „java“.

The backend services interact with the client side of the software implemented using Angular web-framework. This part uses several HTML based web-form to get input parameters for the calculations. An example of such form for polynomials modular multiplications is shown in Figure 2.

The major part of the preliminary calculations of RNS parameters includes formation of the RNS moduli system. A working base of irreducible polynomials is taken from the preliminary formed database of irreducible polynomials. These polynomials are chosen randomly according

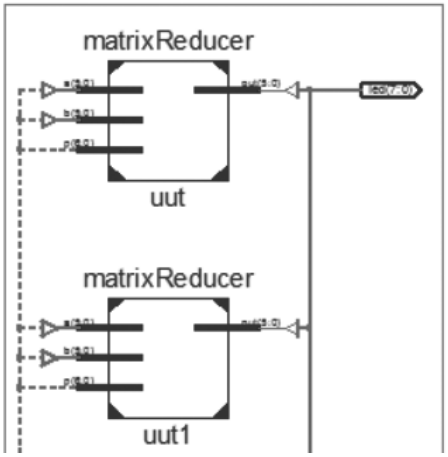


Fig. 5. Fragment of the top-level module of the circuit

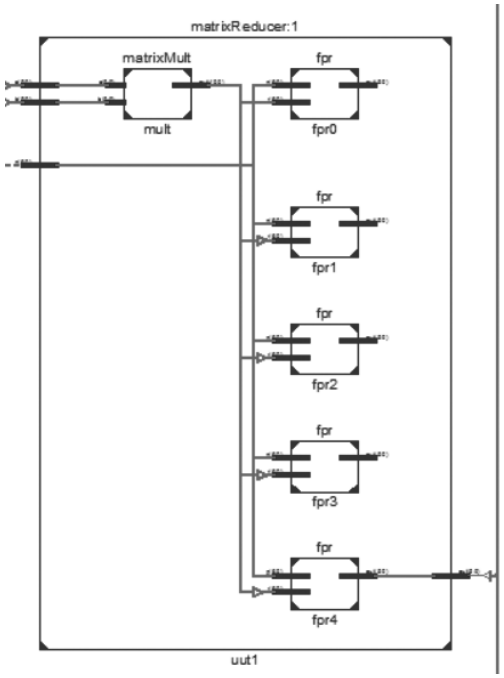


Fig. 6. The structure of a single multiplier modulo irreducible polynomials

to provided degrees to fill the length of the input data block as described in [7]. Number of irreducible polynomials and their degrees are provided through the inputs shown in Figure 3.

3. Interaction with the hardware part of the system. A work is being done to develop and implement a software-hardware system for preliminary calculation of the parameters of the non-position number system. In this implementation, the main time-consuming operation — division of a polynomial modulo an irreducible polynomial — is performed hardware-wise on a multiplication device, the scheme of which was presented in [8].

The hardware platform is FPGA Artix-7 (XC7A35TICSG324-1L) based on the Arty A7 development board from Digilent [9].

In the software part of this work, the Microblaze microprocessor core implemented on the basis of Xilinx FPGA is used. MicroBlaze is an integral part of the Embedded Development

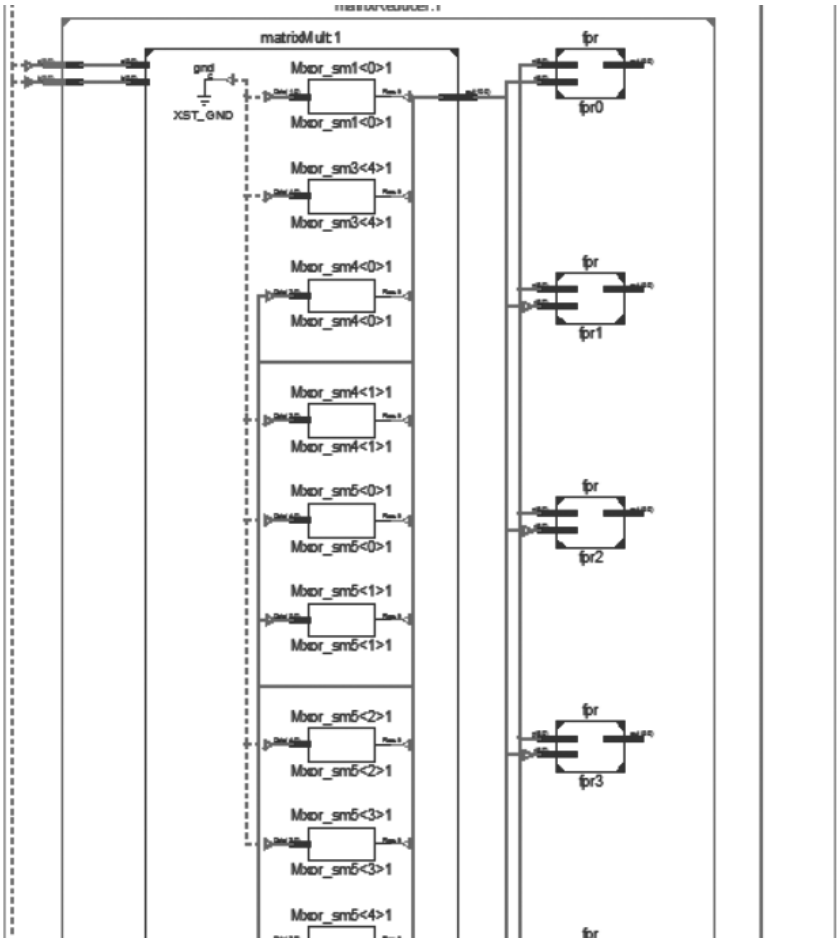


Fig. 7. The structure of an adder tree and PRFs

Kit (EDK) package, offered by Xilinx as the main tool for developing and debugging embedded FPGA-based microprocessor systems.

Elements of the MicroBlazeprocessor family are embedded microprocessor cores with RISC architecture, which are designed for use on FPGA base systems. The scheme of the processor and periphery devices is shown in Figure 4.

The polynomial data for multiplication is prepared on the MicroBlaze microprocessor, and then this data is transferred to the multiplier device to be multiplied by a modulo of an irreducible polynomial.

4. Design of a hardware multiplier for the nonpositional cryptosystem. Hardware encryption has a number of significant advantages over software encryption [10]: encryption has a higher speed; hardware implementations of cryptographical algorithms guarantee their integrity; on the basis of hardware encryptors it is possible to create a system for protecting information from unauthorized access and distinguishing access to a computer; the use of a specialized cryptographic processor for performing cryptographic transformations unloads the central processor of the computer.

Currently a research project on the hardware implementation of the considered cryptosystem is in progress. As was shown above, the main advantages of using the nonpositional number system are the absence of transfer of bits in the operations of addition and multiplication,

and, consequently, the possibility of parallel execution of operations on each of the bases of the system, which significantly speeds up the calculation process.

During routine calculations in NPNS the main hardware unit is a device for multiplying polynomials modulo irreducible polynomials with coefficients in GF (2). Considering the foregoing, the development of a hardware multiplier for the NPNS is a relevant task, the solution of which will provide opportunities for creating effective hardware implementations cryptosystems based on a polynomial RNS.

Let consider the initial polynomial multiplier scheme using the classical approach of building a multiplier — the product of polynomials is calculated by summing the rows of matrices of the partial product on multilevel adders, and the modular reduction is performed on „partial residue formers“ (PRF). To sum the rows of the matrix, partial products in rows are grouped by pairs and each pair is summed in parallel on the adder by modulo two, forming the first-level adder. Further, the results of addition, which were obtained at the first level, are also grouped in pairs and summed on the adder by modulo two, forming second-level adders. Such a summation is processed until the result is obtained. Thus, the formation of the product of polynomials occurs on the tree of adders, which has several levels. The number of levels and adders at each level depends on the bit capacity of the multiplied polynomials.

The developed design is to be implemented in HDL Verilog language and synthesized using the Xilinx Artix-7 FPGA. The circuit description consists of the following components: the top-level module (Figure 5). In this module, the multipliers (matrixReducer), their inputs and outputs are defined. Each module of the matrixReducer multiplier consists of a module of matrix row conjunctures, an adder tree and PRF modules (Figure 6). The general structure of the connection of the adder tree and PRF modules is shown in Figure 7.

Conclusion. At present, RNS is often used to develop efficient and high-performance special purpose processors [11], which are widely used, in cryptography [12, 13].

The ongoing research is aimed for the development of algorithms for multiplying polynomials modulo irreducible polynomials, the synthesis and implementation of various digital multiplier circuits on their basis for the purpose of the software-hardware implementation of symmetric cryptosystems based on the nonpositional number system. The developed modular multiplier is planned to be used as a main calculation unit during hardware implementation of the proposed encryption systems built on NPNS so that calculation in the residue number system can be performed more efficiently in hardware.

In the developed multiplier, the product of polynomials is calculated by summing the rows of matrices of the partial product using multilevel tree of adders. After that a modular reduction by irreducible polynomial is performed.

The application of the non-positional number system allows accelerating slow calculations in asymmetric encryption algorithms and increasing their reliability as well.

References

1. Gura N. „Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs “ Proc. 6th Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES 04) LNCS 3156. Springer, 2004. P. 119–132.

2. Kumar S. Elliptic Curve Cryptography for Constrained Devices, doctoral dissertation, Electrical Engineering and Information Sciences. Bochum: Germany; Ruhr University, 2006.

3. Omondi, B. Premkumar, Residue Number Systems: Theory and Implementation, 2007.

4. Biyashev R., Nyssanbayeva S. Algorithm for Creation a Digital Signature with Error Detection and Correction // Cybernetics and Systems Analysis. 2012. V. 48. № 4. P. 489–497.

5. Kalimoldayev M., Nyssanbayeva S., Magzom M. Model of nonconventional encryption algorithm based on nested Feistel network // Open Engineering. 2016. № 6. P. 225–227.

6. Biyashev R., Kalimoldayev M., Nyssanbayeva S., Magzom M. Development of an encryption algorithm based on nonpositional polynomial notations // Proceedings of the International Conference on Advanced Materials Science and Environmental Engineering (AMSEE 2016). Chiang Mai, Thailand, June 26– 27, 2016. P. 243–245.

7. Biyashev R., Nyssanbayeva S., Begimbayeva Ye., Magzom M. Building modified modular cryptographic systems // International Journal of Applied Mathematics and Informatics. 2015. V. 9. P. 103–109.

8. Tynymbayev S., Kapalova N., Magzom M. Development and implementation of a hardware multiplier in the non-position numeral system (in Russian) // Proceedings of IICT conference „Modern problems of computer science and computer technologies“. Almaty, 2017. P. 263–270.

9. Arty A7: Artix-7 FPGA Development Board for Makers and Hobbyists. [El. Res.]: https://store.digilentinc.com/arty-a7-artix-7-fpga-development-board-for-maker s-and-hobbyists/ (may 2018).

10. Acosta A., Addabbo T., Tena-Sбnchez E. Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview // Int. J. Circ. Theor. Appl. 2017. № 45. P. 145–169.

11. Rooju Chokshi, Krzysztof S. Berezowski, Aviral Shrivastava, Stanisiaw J. Piestrak. Exploiting Residue Number System for Power-Efficient Digital Signal Processing in Embedded Processors // Proceedings of the CASES '09, Grenoble, France, P. 19–28.

12. Schinianakis D., Stouraitis T. Residue Number Systems in Cryptography: Design, Challenges, Robustness // Secure System Design and Trustable Computing. Springer, 2016.

13. Sousa L., Antro S., Martins P. Combining residue arithmetic to design efficient cryptographic circuits and systems // IEEE Circuits and Systems Magazine, 2016.

Калимолдаев Максат Нурадилович — академик НАН РК, доктор физико-математических наук, профессор Института информационных и вычислительных технологий КН МОН РК, г. Алма-Ата, Республика Казахстан; тел.: +77072107379, e-mail: mnk@ipic.kz.

Калимолдаев Максат Нурадилович, академик НАН РК, доктор физико-математических наук, профессор. Генеральный директор Института информационных и вычислительных технологий КН МОН РК. Руководитель проекта „Разработка программно-аппаратных средств для криптосистем на базе непозиционной системы счисления“. Научные интересы: информационная безопасность, разработка и создание средств многоуровневого разграничения доступа к данным; математическое моделирование и управление динамическими, техническими и экономическими системами. В 2015–2017 гг. руководитель проекта программно-целевого финансирования МОН РК 0128/ПЦФ „Разработка и исследование моделей национального алгоритма шифрования на базе модулярной арифметики“, руководитель проекта 3314/ГФ4 „Математическое моделирование, разработка, исследование и реализация методов решения задач динамической оптимизации большой размерности на современной высокопроизводительной вычислительной технике“.

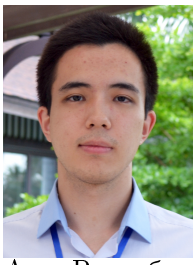
Maksat N. Kalimoldaev, academician of the National Academy of Sciences of the Republic of Kazakhstan, doctor of physical and mathematical sciences, professor. General director of the Institute of Information and Computational Technologies SC MES RK.Scientific interests: information security, development and creation of means of multilevel delimitation of access to data; mathematical modeling and management

of dynamic, technical and economic systems.In 2015–2017 was supervisor of the program-targeted funded project of MES RK 0128/PTF „Development and study of models of the national encryption algorithm based on modular arithmetic“. Supervisor of the project „3314/ГФ4 Mathematical modeling, development, research and realization of methods for the solution of problems of dynamic optimization of large dimensionality on the modern high-performance computing equipment“.

Тынымбаев Сахыбай — канд. технич. наук, доцент, главный научный сотрудник Лаборатории информационной безопасности Института информационных и вычислительных технологий КН МОН РК, г. Алма-Ата, Республика Казахстан. Тел.: +77756363840, s.tynym@mail.ru.

Тынымбаев Сахыбай — канд. техн. наук, доцент. Соруководитель проекта „Разработка программно-аппаратных средств для криптосистем на базе непозиционной системы счисления“. Основные направления научной деятельности: операционные устройства вычислительной техники и криптосистем. В 2015–2017 гг. руководитель инициативной научно-исследовательской работы „Анализ и разработка структур основных операционных блоков асимметричных криптоалгоритмов“.

Sakhybay Tynymbayev, candidate of technical sciences, professor.Co- supervisor of the project „Development of software-hardware facilities for cryptosystems based on the nonpositional number system“. The direction of his scientific interests is related to the development of hardware for various digital systems. In 2015–2017 was supervisor of the initiative research work „Analysis and development of the structures of the main operating blocks of asymmetric crypto algorithms“.



Магзом Мирас Мухтарулы – старший научный сотрудник Лаборатории информационной безопасности Института информационных и вычислительных технологий КН МОН РК, г. Алма-Ата, Республика Казахстан; доктор PhD; тел.: +77078878246.

Мирас Магзом получил степень магистра технических наук по специальности „Вычислительная техника и программное обеспечение“ в 2014 году в Алматинском университете энергетики и связи. С 2014 года проходил обучение по совместной программе PhD в Институте информационных и вычислительных технологий МОН РК и Казахском национальном университете им. Аль-Фараби по специальности „Вычислительная техника и программное обеспечение“. С 2015 года работает в лаборатории информационной безопасности Института информационных и вычислительных технологий. В 2017 году получил степень PhD.

Miras Magzom received his M.S. degree in Computer Science in 2014 from Almaty University of Power Engineering and Telecommunications. Since 2014 studied PhD in Computer Science by the joint program in Institute of Informational and Computational Technologies of Ministry of Education and Science of the Republic of Kazakhstan and Al-Farabi Kazakh National University. Since 2015 works in the Laboratory of Informational Security in Institute of Informational and Computational Technologies. Received his PhD degree in 2017.

Дата поступления — 12.09.2018