УДК 004.056.5

Oleksandr Markovskyi, Masimyk Viktoria,
Kot Olga, Kuts Volodymyr.

THE EMPLOYMENT OF MONTGOMERY REDUCTION FORACCELERATION OF EXPONENT ON GALOISE FIELDS CALCULATION

The paper proposes an approach to acceleration of the calculation of the Galois field exposure operation, which is important for cryptographic data protection, based on a modification of Montgomery technology. The methods of multiplication and exponentiation in Galois fields with the Montgomery reduction of intermediate results are proposed. It is shown that the use of modified Montgomery technology allows to accelerate the calculation of the exponent in the Galois fields 5 .5 times.

Keywords: Galois fields, public key cryptographic algorithms, Montgomery reduction.

Tabl.: 1. Bibl.: 4.

Acute problem. The development of cloud technologies is endowed with a wide range of users, and before they are potential attackers, available for significant for existing computing power. This, before the work of people, reduces the level of security of different groups of cryptographic data and requires adequate measures. For public key algorithms, the level of security can be increased by increasing the bit size of numbers. But this results in a significant slowdown in the implementation of calculations associated with the realization of these algorithms. Therefore, there is a need to compensate this by the developing of new methods to accelerate the calculation of the exponent in the Galois fields, which underliesin a wide range of mechanisms for cryptographic protection of information[1]

Target setting. An alternative to traditional algebra is the use of Galois finite fields, the exposition of which is realized an order of magnitude faster. However, this algebra does not use Montgomery technology, which focuses on traditional algebra. Accordingly, there is a scientific problem of modifying Montgomery technology for Galois field algebra and developing, on this basis, methods of multiplication and exposition using Montgomery reduction to accelerate the calculation of the exponent in finite fields[2].

Actual scientific researches and issues analysis. Acceleration of the calculation of the exponent in the Galois fields can be achieved due to a number of factors. In it was proposed[3] to organize an accelerated calculation of the exponent on the finite Galois fields due to a specific property of the basic exponentiation operation - polynomial squaring, which does not actually require computing resources and is reduced to inserting zeros between binary digits. However, this approach does not reduce the time for reduction of the resulting polynomial square code.

Another known [4] method is based on the invariance of the Galois polynomial-forming field in protection protocols with public keys. This allows you to use pre-calculations that depend entirely on the forming polynomial with preserving the results in the tables. However, this approach does not reduce the reduction time.

Uninvestigated parts of general matters defining. A review of the known solutions to the acceleration of exposition on Galois fields showed that they do not allow to accelerate an important part of the calculations - namely, finding the remainder of the polynomial division of intermediate results by the polynomial-forming field.

The research objective. The aim of the research is to accelerate the calculation of exponents on Galois fields by reducing the time required to reduce intermediate results by modifying the Montgomery technology used to accelerate the reduction in traditional algebra.

The statement of basic materials. The paper proposes an approach to the acceleration of the calculation of the exposition operation on Galois fields, which is important for a wide range of cryptographic data protection algorithms. It is based on a modification of the known Montgomery technology to accelerate the calculation of the remainder of the polynomial division. Based on the developed modification, a method of multiplication on Galois fields with Montgomery reduction of intermediate results of polynomial multiplication is proposed, as well as a method of exponentiation on fields using the developed multiplication scheme.

Method for multiplication in Galois fields using Montgomery reduction. When performing multiplication in finite fields, the polynomial in m-1 power is considered: A(x) $=a_{m-1}\cdot x^{m-1} + a_{m-2}\cdot x^{,m-2} + \ldots + a_1\cdot x + a_0$ and B(x) $= b_{m-1}\cdot x^{m-1} + {} + b_{m-2}\cdot x^{,m-2} + \ldots + b_1\cdot x + b_0$, where $\forall i \in \{0,1,\ldots,m\text{-}1\}$: $a_i, b_i, p_i \in \{0,1\}$. These polynomials A($x$) and B($x$) correlate with m -bit binary numbers A $=a_{m-1}\cdot 2^{m-1} + a_{m-2}\cdot 2^{,m-2} + \ldots + {} + a_1\cdot 2 + a_0$ and B$= b_{m-1}\cdot 2^{m-1} + b_{m-2}\cdot 2^{,m-2} + \ldots + b_1\cdot 2 + b_0$ respectively. The finite field in which the multiplication operation is performed is given by the generating polynomial Q(x) in m power: Q(x)$= q_m\cdot x^m + q_{m-1}\cdot x^{,m-1} + \ldots + q_1\cdot x + q_0$ where $\forall i \in \{0,1,\ldots,m\}$: $q_i \in \{0,1\}$.

In order to enable, according to Montgomery technology, reduction of a complex polynomial division operation to the Montgomery recursion procedure developed above, it is necessary to use an auxiliary polynomial in m power $U(x)= x^m$. This auxiliary polynomial corresponds to an integer U$=2^m$. For an auxiliary polynomial, its multiplicative inversion can be determined according to the known algorithms, ie the polynomial $\mathrm{U}^{-1}(\mathrm{x})$, polynomial multiplication of which by the auxiliary polynomial in the field formed by the polynomial Q(x) gives 1:

$\mathrm{U}(x)\otimes \mathrm{U}^{-1}(x)$ rem Q(x) = 1.

As a result of Montgomery polynomial multiplication there should be formed the polynomial product of polynomials P(x) =$p_{m\text{-}1}\cdot x^{m\text{-}1}$ + $p_{m\text{-}2}\cdot x^{,m\text{-}2}$ + …+ $p_1\cdot x$+ p_0 in m-1 power. Polynomial of a product when using Montgomery technology is actually a polynomial product of polynomials A(x) and B(x) and the polynomial of the multiplicative inversion $U^{-1}(x)$ reduced to the field with the generating polynomial Q(x): $P(x)$ = (A(x)⊗ B(x) ⊗ $U^{-1}(x)$) rem Q(x). Thus, in order to receive the correct result of multiplication in the Galois field the received polynomial P(x) should be multiplied polynomially by the auxiliary polynomial U(x), reducing the result in the Galois field formed by the polynomial Q(x).

The developed procedure for multiplication in Galois fields with result reduction using Montgomery technology can be described by the following meaningful algorithm:

1) Specify the starting value of the result P as zero: P=0. Set the counter of i cycles, which is also the number of the current digit of the multiplier, also as zero: i=0.

2) Perform a logical addition (addition according to the module two) of the code of multiplicand A to the current value of the result P: P = P ⊕ A if the current digit of the multiplier b_i is equil to 1.

3) Test the least significant bit of the code of the current result P: if the least significant bit p_0 of the current result is equal to 1, then the current value P of the number Q, which corresponds to the generaing polynomial Q(x) of the Galois field: P = P ⊕□Q should be logically added (addition according to module two) to the code. Since the least significant digit q_0 of Q is always equal to 1 (otherwise the generating polynomial Q(x) would not be prime), that means that after the described operation, the least significant p_0 of the current result is exactly equal to zero.

4) A logical shift to the right by one position of the code of the current result P is performed: P = SHR(P). Since the least significant digit p_0 of the code of the current result P is exactly equal to zero, that means that nothing is lost in the resut of such a shift.

5) Increase the counter of i cycles by one, which is also the number of the current digit of the multiplier: i=i+1. Repeat the algorithm of the point 2 if the value of the counter after this operation is less than the m power of the generating polynomial.

6). Compare the code P of the current result and the number Q, which correlates with the generating polynomial Q(x) of the Galois field: if P ≥ Q, then the current value P of the number Q, which is correlated with the generating polynomial Q(x) of the Galois field: P = P ⊕ Q should be logically added (addition according to the module two) to the code.

7) The end of the algorithm. The result of Montgomery multiplication in the Galois field with the generating polynomial Q(x) is fixed in the variable of the current result P, the value of which is equal to (A⊗ B ⊗ U^{-1}) rem Q.

The proposed Montgomery multiplication algorithm in Galois fields can be illustrated in the following example. Let the power m of the generating polynomial of Galois field be five: that is, m = 5, the generating polynomial Q(X) has the following form: $Q(x)=x^5+x+1$. This generating polynomial corresponds to the number Q=19. Based on the value of the power of the Galois field generating polynomial, the auxiliary polynomial U(x)=x^5 is chosen . This polynomial corresponds to the number $U=2^5=32$. According to Euclid's algorithm, it is determined by the polynomial of multiplicative inversion $U^{-1}(x)$ = = x+1. The last polynomial corresponds to the number $U^{-1}=3$.

In the example of Montgomery multiplication in the Galois field considered, the number of numbers $A=17_{10}=10001_2$ is a multiplier, and the number B, which is equal to 11: $B=11_{10} = 1011_2$ is a multiplicand.

Table 1 shows the sequence of values of the parameters of the above specified Montgomery multiplication algorithm in the Galois fields in order of cycles of its perorming.

Table 1

Sequence of values of variables of algorithm in the order of cycles of its performing for values A=17 and B=11

i	b_i	**Поточний результат P**				
		At the beginning of the cycle	**After adding a multiplicand**	p_0	**After adding a module**	**After shift**
0	1	0	0+17 = 17	1	17+19= 36	18
1	1	18	18+17= 35	1	35+19 =54	27
2	0	27	27	1	27+19= 46	23
3	1	23	23+17= 40	0	40	20
4	0	20	20	0	20	10

The recceived result P=10 corresponds to the (A⊗B⊗U^{-1}) rem Q = (17⊗11⊗3) rem 19 = 10.

Exponentiation method in Galois fields using Montgomery reduction. Exponentiation in Galois fields using Montgomery recursion presupposes calculating of A^E rem Q without polynomial division operations for reduction implementing, ie finding the remainder of the polynomial division.

When performing exponentiation in finite fields, a polynomial in the m -1 power should be used: Q(x)= $q_m\cdot x^m + q_{m-1}\cdot x^{,m-1} + \ldots + q_1\cdot x + q_0$, where $\forall i\in\{0,1,\ldots,m\}$: $q_i\in\{0,1\}$. The specified polynomial A(x) correlates with the m-bit binary number

A=$a_{m-1}\cdot 2^{m-1}$ + $a_{m-2}\cdot 2^{,m-2}$ + …+ $a_1\cdot 2$+ a_0. The finite field in which the exponentiation operation is performed should be defined by the generating polynomial Q(x) in m power: Q(x)= $q_m\cdot x^m$ + $q_{m-1}\cdot x^{,m-1}$ + …+ $q_1\cdot x$+ q_0 where $\forall i\in\{0,1,\ldots,m\}$: $q_i\in\{0,1\}$. The generating polynomial can also be unambiguously assigned m -bit binary number Q= $q_m\cdot 2^m$ + $q_{m-1}\cdot 2^{,m-1}$ + …+ $q_1\cdot 2$+ q_0. In order to enable, according to Montgomery technology, reduction of a complex polynomial division operation to the Montgomery recursion procedure developed above, it is necessary to use an auxiliary polynomial in m power $U(x)$= x^m. This auxiliary polynomial corresponds to an integer U=2^m. For an auxiliary polynomial, its multiplicative inversion can be determined according to the known algorithms, ie the polynomial U^{-1}(x), polynomial multiplication of which by the auxiliary polynomial in the field formed by the polynomial Q(x) gives 1: U(x)⊗U^{-1}(x) rem Q(x) = 1. The exponent code consists of v binary digits: E=(e_v e_{v-1} …. e_0 $)_2$, where e_v= 1 and v<m.

Calculations are performed preliminarily, and their results depend only on the module Q(x): the initial value of the current result R= U rem Q(x), and D= U^2 rem Q(x). The described above method of multiplication in Galois fields with Montgomery reduction is used in the proposed procedure. The actions performed by this method are conventionally indicated in the description of the exponentiation procedure through PM(x,y).

The proposed procedure of modular exponentiation using Montgomery recursion, ie the calculation of $A/^E$ rem Q(x) presupposes the following sequence of actions:

1. First, determine the product in the Galois field that is formed by the polyomial Q(x), of the A number, raised to the power of E, by the auxiliary variable of the D algorithm. The result is stored in a variable C: C=PM(A,D).

2. The indicator i of the current digit of the exponent code is set by the maximum value v: i=v, where this indicator points the most significant (ie single) digit of the exponent code e_v .

3. The current result, which is stored in the variable R, is multiplied by itself in the Galois field using the developed multiplication procedure based on the Montgomery reduction: R = PM(R,R).

4. If the current i -th bit of the code of the exponent E is equal to 1: e_i = 1, then the current result is multiplied by the value of the variable C: R=PM(R,C).

5. The analysis of the current value of the indicator is performed: if i > 0, then i is reduced by one: i=i-1 with the following repeating of actions specified in point 3.

6. The final result of exponentiation in the Galois field is formed by multiplying the value of the current result in the variable R by one: R = PM(R,1).

Conclusions. It is theoretically and experimentally proved that the use of Montgomery technology allows to accelerate 5.5 times the computational implementation of multiplication and, accordingly, exposition on finite Galois fields. Acceleration is achieved due to two main factors: halving the number of digits processed in the reduction process and replacing the polynomial division operation with a simpler computational shift operation. Inherent in the Montgomery technology, the operation of correcting the result is performed only once every 2048 cycles and has virtually no effect on the rate of calculation of the exponent on the Galois fields.

References

1. Markovskyy, O.P Galois fields algebra utilization for implementation of the conception of zero-knowledge under identification and authentication of remote users/Zacharioudakis Leftherios, Maksymuk V.R.. // Electronic modeling. Collection of scientific works: V 6(39).- 2017.- P.33-45.

2. Montgommery P.L. Modular multiplication without trial division / P.L. Montgommery // Mathematics of Computation. — 1985— Vol. 44. — P. 519-521.

3. Koc C.K. Analyzing and comparing Montgomery Multiplication Algorithms./ C.K. Koc, Acar T., Kaliski B.S. // IEEE Micro. —1996 — V.16, № 3. — P. 26— 33.

4. Samofalov KG Methods of accelerated implementation of exponentiation in Galois fields in the information protection system / Markovsky OP, Sharshakov AS // Problems of information information and management. Collection of scientific works: K., NAU. - 2011. - Vol.2, № 33 - P.143-151.

AUTHORS

Oleksandr Markovskyi (supervisor) – Associate Professor, PhD, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

Viktoriia Maksymuk – student, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

Olha Kot– student, Department of Computer Engineering, National
Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

Volodymyr Kuts– senior lecturer, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”