УДК 681.142

С.О.МАРТЫНЕНКО, В.А. КРАСНОБАЕВ

Харьковский национальный технический университет сельского хозяйства имени Петра Василенко, Украина

МЕТОД ВОЗВЕДЕННЯ ЧИСЕЛ В КВАДРАТ ПО МОДУЛЮ М МОДУЛЯРНОЙ СИСТЕМЫ СЧИСЛЕНИЯ

На основе принципов реализации модульных операция в теории чисел, предложен метод возведения чисел в квадрат по модулю, на основе которого разработаны устройства для его реализации.

Ключевые слова: *модулярная система счисления, модульные операции, возведение в квадрат.*

Введение

Часто при криптографических преобразованиях возникает задача возведения числа (элемента) А в квадрат по модулю m, т. е. задача определения выражения $A^2(\text{mod } m)$. Так, для базиса расширенного поля (нормального базиса) не обходимо производить операцию возведения в квадрат элемента А. При построении эллиптической кривой над простым полем Галуа и при ее описании требуется введение в теорию модулярных форм и функций, квадратичных полей и функций Вейерштрасса.

При решении уравнения Фробениуса для подгруппы значительная часть вычислений состоит в расчете значений $x^m, x^m, x^{m^2}, y^{m^2}$ в заданном кольце. Экспоненцирование производится обычным методом последовательных возведений чисел в квадрат и умножений по модулю m.

Таким образом актуальны исследования, посвященные поискам методов реализации операции $A^2 \text{ (mod } m)$, позволяющие уменьшить временные и аппаратные затраты. Это позволит уменьшить вычислительную сложность криптографического алгоритма.

Обзор литературных источников. При построении эллиптической кривой и расчете ее порядка требуется произвести $N_к$ операций возведения в квадрат [1 - 3].

При расчете порядка эллиптической кривой используются процедуры Р. Скуфа [4, 5] с последующей модификацией А. Эткина [6, 7], Н. Илкиса [8, 9] и Т. Сато [10]. Во всех процедурах используется китайская теорема об остатках с обязательным вычислением заданного $N_и$ числа инверсий, заданного числа $N_к$, заданного числа $N_у$ умножений при сложении и удвоении точек соответственно а аффинных (А), проективных (П), якобиановых (Я) координатах, а также в координатах Чудновского (Ч), и модифицированных якобиановых (МЯ) координатах.

В табл. 1 представлено число операций $N_у$ умножения, число $N_к$ возведения в квадрат и число $N_и$ проведенных инверсий элементов простого поля при сложении и удвоении точек в различных координатных системах.

Таблица 1

Количество операций криптопреобразования

Координаты	Операция сложения точек	Операция удвоения точек
А	$N_и + 2 \cdot N_у + N_к$	$N_и + 2 \cdot N_у + 2 \cdot N_к$
П	$12 \cdot N_у + 2 \cdot N_к$	$7 \cdot N_у + 5 \cdot N_к$
Я	$12 \cdot N_у + 4 \cdot N_к$	$4 \cdot N_у + 6 \cdot N_к$
Ч	$11 \cdot N_у + 3 \cdot N_к$	$5 \cdot N_у + 6 \cdot N_к$
МЯ	$13 \cdot N_у + 6 \cdot N_к$	$4 \cdot N_у + 4 \cdot N_к$

По некоторым оценкам [1, 2] одна операция инверсий равна $N_и \approx 80\ N_у$, а одна операция $N_к \approx 0{,}8\ N_у$ (при операциях в простом поле Галуа). Из таблицы видно, что во всех перечисленных процедурах возникает необходимость реализовать операцию $A^2(\text{mod } m)$.

Цель статьи – разработать метод реализации операции $A^2 \text{ (mod } m)$ возведения чисел А в квадрат по модулю m, а также на его основе синтезировать устройства для его реализации.

Основная часть

Пусть необходимо определить значения $A^2 \text{ (mod } m)$, где: А, m – натуральные числа и $0 \le A \le m - 1$. Покажем, что выполняется следующее математическое равенство

$$A^2 \text{ (mod } m) = (m - A)^2 \text{ mod } m. \qquad (1)$$

Пусть A^2 представим в виде $A^2 = k \cdot m + \alpha$ ($0 \le \alpha \le m - 1$), т. е. $A^2 \equiv \alpha \pmod m$. Тогда $(m - A)^2 = m^2 - 2 \cdot m \cdot A + A^2 = m^2 - 2 \cdot m \cdot A + k \cdot m + \alpha$. В этом случае $(m^2 - 2 \cdot m \cdot A + k \cdot m + \alpha) \equiv \alpha \pmod m$. Данное равенство справедливо для m четного и нечетного. В случае технической реализации операции $A^2 \pmod m$ целесообразно рассмотреть три возможных варианта значения m.

Первый вариант для $m = 2 \cdot n + 1$ нечетного ($n = 0, 1, 2, \ldots$). В этом случае схема организации реализации операции $A^2 \pmod m$ представлена на рис. 1. Данная схема представлена в общем виде и реализует алгоритм, представленный выражением (1). Схема работает следующим образом. По входу устройства во входной регистр в двоичном коде записывается число A. С выхода дешифратора число A, в унитарном ходе, через соответствующий логический элемент ИЛИ (в соответствии с алгоритмом (1)) поступает на вход шифратора, который соответствует значению $A^2 \pmod m$. С выхода шифратора значение $A^2 \pmod m$ в двоичном коде поступает в выходной регистр. Очевидно, что основным звеном технической реализации операции $A^2 \pmod m$ является кодировка шин между дешифратором и шифратором. Для более подробного пояснения алгоритма функционирования основного звена технической реализации $A^2 \pmod m$, он представлен в табл. 2 для $m = 11$.

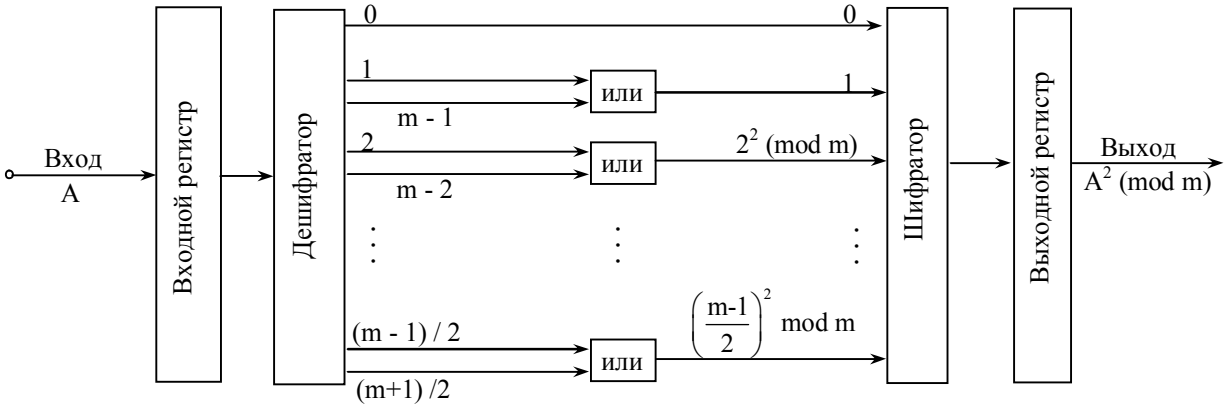

Рис. 1. Первый вариант схемы, реализующей операцию $A^2 \pmod m$

Таблица 2

Алгоритм образования результата $A^2 \pmod m$ операции (первый вариант)

Номер пары выходных шин дешифратора	Значения, присваиваемые паре выходных шин дешифратора	Значения $A^2 \pmod{11}$, которые присваиваются входным шинам шифратора	Значения выходных шин шифратора
0	0	0	0000
1	1,10	1	0001
2	2,9	4	0100
3	3,8	9	1001
4	4,7	5	0101
5	5,6	3	0011

Второй вариант для $m = 2n$ четного и $m/2$ также четного чисел. В этом случае $\frac{m}{2}$ целое число и, следовательно, $\left(\frac{m}{2}\right)^2 = \frac{m}{4} \cdot m \equiv 0 \pmod m$.

Тогда выходная шина дешифратора, соответствующая значению m/2, одновременно с нулевой шиной, через нулевой элемент ИЛИ подключена к нулевому входу шифратора.

Таким образом алгоритм функционирования устройства, в соответствии со вторым вариантом, определяется следующим математическим соотношением

$$\left(\frac{m}{2}\right)^2 = 0 \pmod m \qquad (2)$$

В этом случае схема организации процесса реализации операции $A^2 \pmod m$ представлена на рис. 2. В табл. 3 представлен алгоритм образования численного значения $A^2 \pmod m$ для m = 12 (m/2 = 6).

Третий вариант для m = 2 · n четного и m/2 нечетного чисел. Для данного варианта выполняется условие

$$\left(\frac{m}{2}\right)^2 \equiv \frac{m}{2} \pmod m \qquad (3)$$

Действительно выражение (3) легко представить в виде

$$\frac{m}{2}\cdot\left(\frac{m}{2}-1\right) = 0 \pmod{\frac{m}{2}\cdot 2}. \qquad (4)$$

Из теории чисел известно, что сравнимость A ≡ B (mod m) двух чисел A и B по модулю m равносильна делимости числа A – B на модуль m. Из выражения (4) следует, что число $\frac{m}{2}\cdot\left(\frac{m}{2}-1\right)$ делится на модуль $m=\frac{m}{2}\cdot 2$.

Действительно, первое слагаемое $\frac{m}{2}$ произведения (4) делится на $\frac{m}{2}$, а второе $\frac{m}{2}-1$ слагаемое – делится на два, так как по условию $\frac{m}{2}$ нечетное число.

Таким образом показана справедливость сравнения (3).

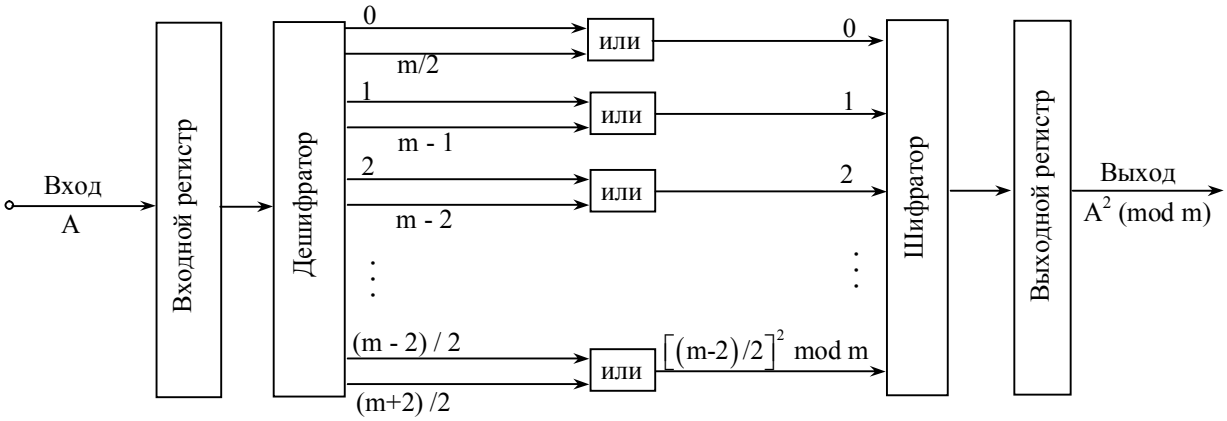

Рис. 2. Второй вариант схемы, реализующей операцию $A^2 \pmod m$

Таблица 3

Алгоритм образования результата $A^2 \pmod m$ операции (второй вариант)

Номер пары выходных шин дешифратора	Значения, присваиваемые паре выходных шин дешифратора	Значения $A^2 \pmod{12}$, которые присваиваются входным шинам шифратора	Значения выходных шин шифратора
0	0,6	0	0000
1	1,11	1	0001
2	2,10	4	0100
3	3,9	9	1001
4	4,8	4	0100
5	5,7	1	0001

В этом случае выражение (3) является алгоритмом определения значения $A^2 \pmod m$.

Схема организации процесса реализации операции возведения чисел A в квадрат по модулю m представлена на рис. 3. В табл. 4 представлен алгоритм образования значения $A^2 \pmod m$ для модуля m = 14 (m/2 = 7).

На рис. 4 представлены общие схемы объединения выходных шин дешифратора для первого ($ДШ_1$), второго ($ДШ_2$) и третьего ($ДШ_3$) вариантов реализации рассматриваемой операции, а на рис. 5 представлена схема объединения выходных шин дешифратора для первого (m_1 = 11), второго (m_2 = 12) и третьего (m_3 = 14) вариантов. В этом случае схема

реализации операции возведения чисел в квадрат по модулю m МСЧ для произвольного значения модуля будет содержать три дешифратора, четыре группы элементов ИЛИ и три шифратора (рис. 6).

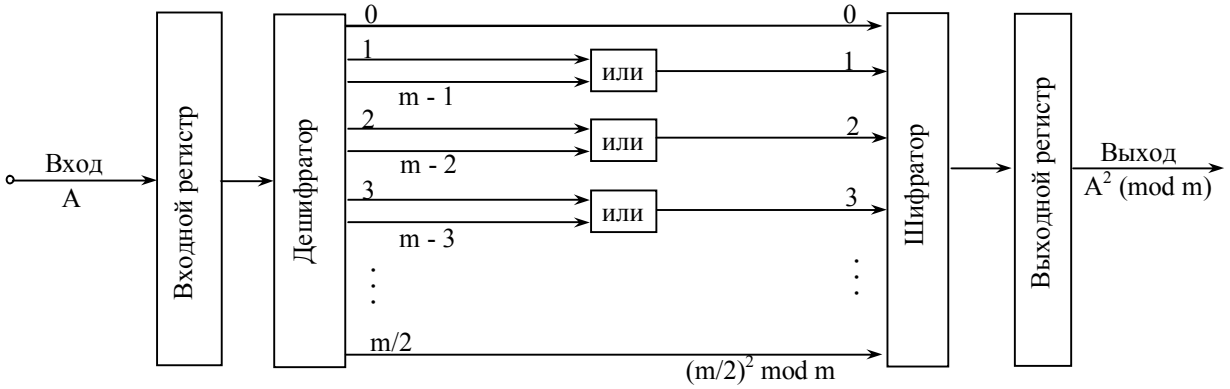

Рис. 3. Третий вариант схемы, реализующей операцию A^2 (mod m)

Таблица 4

Алгоритм образования результата A^2 (mod m) операции (третий вариант)

Номер пары выходных шин дешифратора	Значения, присваиваемые паре выходных шин дешифратора	Значения A^2 (mod 14), которые присваиваются входным шинам шифратора	Значения выходных шин шифратора
0	0,6	0	0000
1	1,13	1	0001
2	2,12	4	0100
3	3,11	9	1001
4	4,10	2	0010
5	5,9	11	1011
6	6,8	8	1000
7	7	7	0111

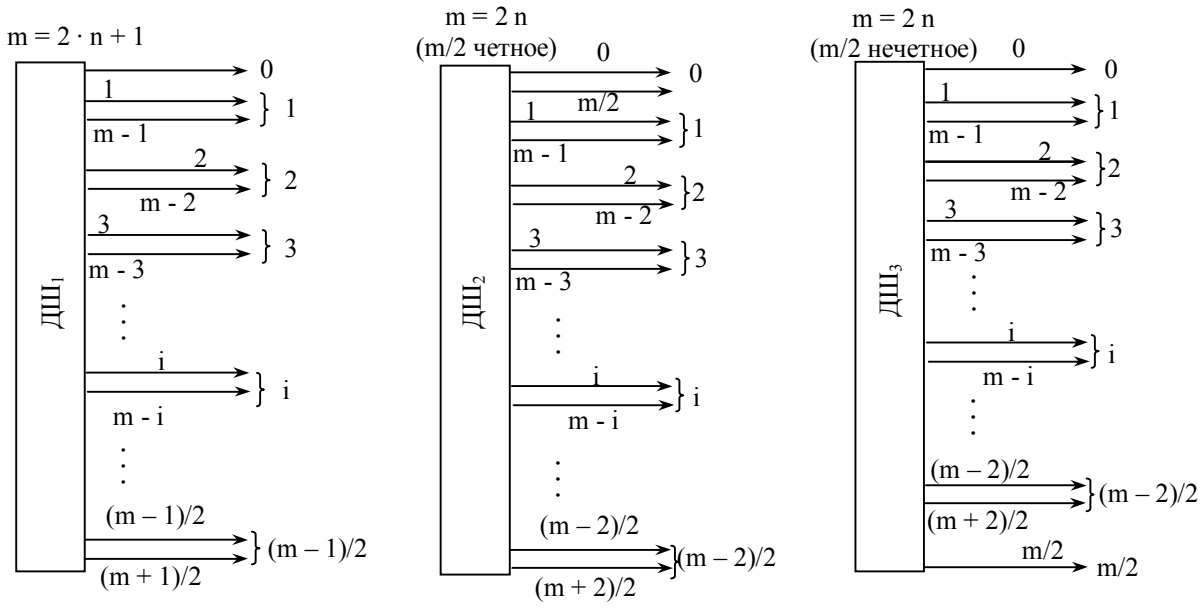

Рис. 4. Схемы объединения выходных шин дешифраторов

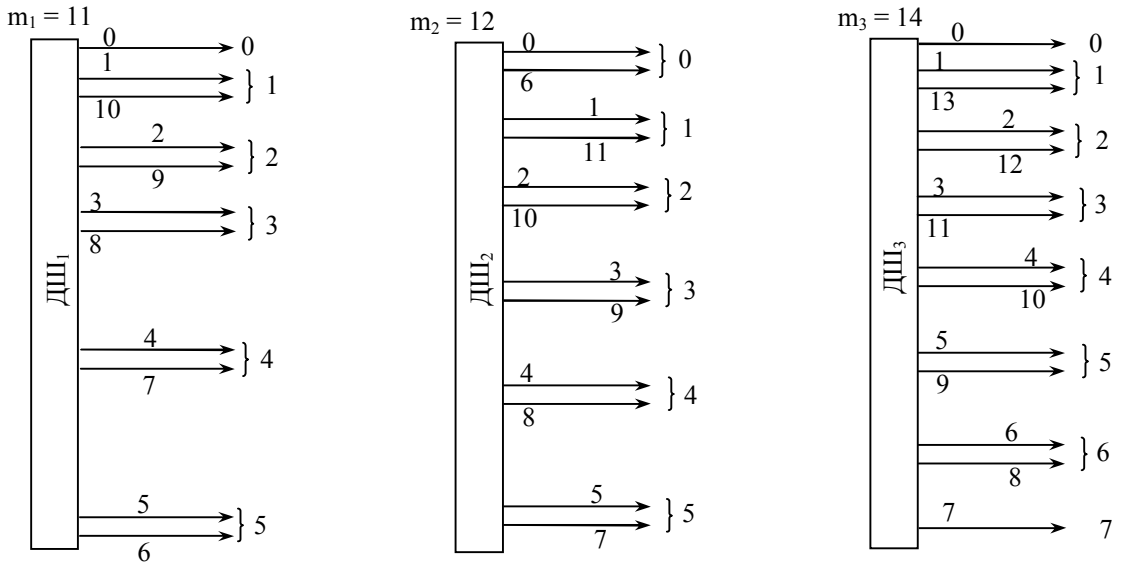

Рис. 5. Схемы объединений выходных шин дешифраторов для $m_1 = 11$, $m_2 = 12$ и $m_3 = 14$

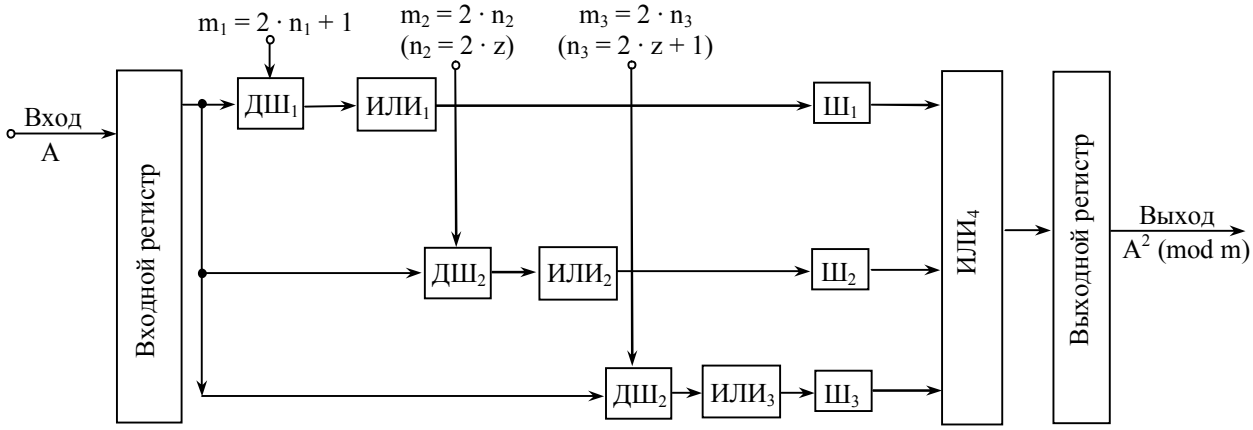

Рис. 6. Схема реализации операции A^2 (mod m) для производного модуля m

Один из недостатков данной схемы – большое количество элементов ИЛИ, непосредственно участвующих в образовании результата A^2 (mod m) операции (первая, вторая и третья группы элементов ИЛИ). Общее количество элементов ИЛИ трех групп ($ИЛИ_1$, $ИЛИ_2$ и $ИЛИ_3$) примерно равно

$$N_{ИЛИ}^{\Sigma} = N_{ИЛИ_1} + N_{ИЛИ_2} + N_{ИЛИ_3}.$$

При реализации операции A^2 (mod m) возведения чисел A в квадрат по одному из модулей $m_i\ (i=\overline{1,3})$, выбирается нужная схема соединения входов-выходов дешифратор-шифратор.

Проведем расчет и сравнительный анализ количества элементов ИЛИ в трех группах. Пусть для определенности $m_1 < m_2 < m_3$ (три возможных варианта). Тогда можно считать, что $N_{ИЛИ}^{\Sigma} \approx 3 \cdot N_{ИЛИ_3}$.

Если считать, что количество элементов ИЛИ в одной группе равно $\left[\frac{m_3}{2}\right]$, тогда $N_{ИЛИ}^{\Sigma} \approx \left[\frac{3}{2} \cdot m_3\right]$, где $[x]$ - целая часть числа x, его не превосходящая. Учитывая, что $m_3 > m_2 > m_1$, то в качестве одной из трех групп элементов $ИЛИ_i$ $\left(i=\overline{1,3}\right)$ необходимо синтезировать схему для наибольшей $ИЛИ_3$ по количеству элементов ИЛИ группу.

Такая схема представлена на рис. 7, где обозначения "m_i" означают сигнал подачи признака модуля m_i, по которому работает схема.

Пусть $m_1 = 11$, $m_2 = 12$ и $m_3 = 14$ ($m_3 > m_2 > m_1$). В этом случае для общей схемы (рис. 6) количество $N_{ИЛИ}^{\Sigma}$ элементов приблизительно равно

$$N_{\substack{ИЛИ \\ \Sigma}} \approx \left\lceil \frac{m_1}{2} \right\rceil + \left\lceil \frac{m_2}{2} \right\rceil + \left\lceil \frac{m_3}{2} \right\rceil = 5 + 6 + 7 = 18,$$

а для упрощенной схемы (рис. 7):

$$N_{\substack{ИЛИ \\ \Sigma}} \approx \left\lceil \frac{m_3}{2} \right\rceil + N_и = 7 + 3 = 10.$$

Для данного набора модулей $m_i \left(i = \overline{1,3}\right)$ имеем выигрыш в уменьшении количества $N_{\substack{ИЛИ \\ \Sigma}}$ элементов И на ≈ 55 % при сохранении всех функциональных возможностей устройства для определения величины $A^2 \pmod m$.

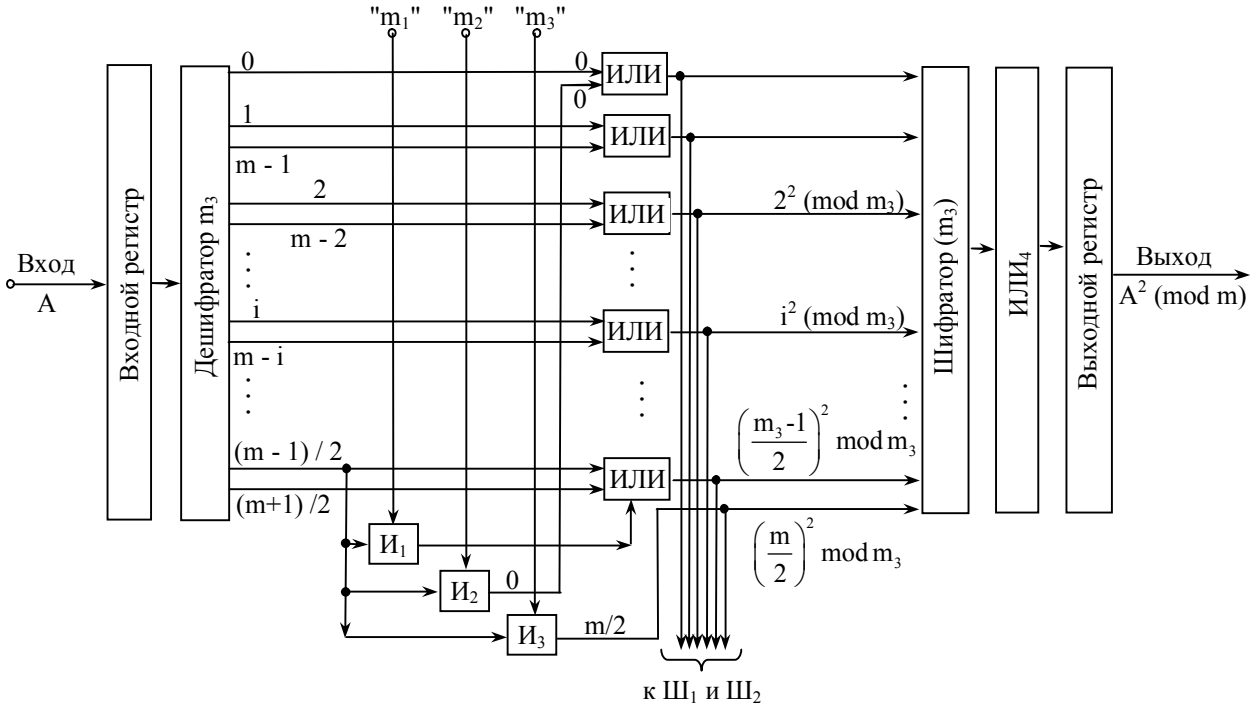

Рис. 7. Обобщенная схема реализации операции $A^2 \pmod m$

Заключение

В данной статье предложен метод возведения чисел в квадрат по модулю m МСЧ. Метод основан на использовании свойств доказанных сравнений (1), (2) и (3). На основании разработанного метода синтезировано три варианта устройств для реализации операции $A^2 \pmod m$ в зависимости от численного значения модуля m. В статье разработано устройство, которое оптимизирует количество оборудования для реализации вышеназванной модульной операции.

Метод рекомендован для использования его при выполнении криптографических преобразований с целью уменьшения их вычислительной сложности.

Литература

1. Brown M. Software Implementation of the NIST Elliptic Curves Over Prime Fields / M. Brown, D. Hankerson, J- Lopez, A. Menezes // Certicom Research, CORR-2000-56, Canada.

2. Hankerson D. Software Implementation of Elliptic Curve Cryptography Over Binary Fields / D. Hankerson, J. Lopez, A. Menezes // Certicom Research, CORR-2000-42, Canada, [Електронний ресурс]. – Режим доступу до ресурсу: www.cacr.math.uwaterloo.ca.

3. Криптосистемы на эллиптических кривых учеб. пособие / А.В. Бессалов, А.Б. Телиженко. – К.: ІВЦ видавництва "Політехніка", 2004. – 224 с.

4. Schoof R. Elliptic curves over finite fields and the computation of square roots mod p / R. Schoof // Mathematics of. Computation. – Vol. 44. – 1985. – P. 483-94.

5. Schoof R. Counting points on an elliptic curve over finite fields / R. Schoof // Proc. Journees Arithmetiques, 93. – Jan., 1995. – P. 219-252.

6. Atkin A.O.L. The number of points on an elliptic curve modulo a prime / A. O. L. Atkin, Draft. – 1988.

7. Atkin A.O.L. The number of points on an elliptic curve modulo a prime (ii) / A.O.L. Atkin, Draft. – 1992.

8. Elkies N.D. Explicit isogenics / N.D. Elkies, Draft. – 1991.

9. Lercier R. Counting the number of points on an elliptic curve over finite fields: strategies and performances / R. Lercier F. Morain // Proc. EUROCRYPT, 95. – P. 101-116.

10. Satoh T. Canonical lifting of elliptic curves and p-adic point counting (theoretical background) / T. Satoh // Departament of Mathematics, Faculty of Science, Saitame University, 2001. – P. 1-21.

Поступила в редакцию 29.01.20010

Рецензент: д-р техн. наук, проф. И.О. Фурман, Харьковский национальный технический университет сельского хозяйства им. Петра Василенка, Харьков, Украина.

МЕТОД ПІДНЕСЕННЯ ЧИСЕЛ ДО КВАДРАТУ ЗА МОДУЛЕМ М МОДУЛЯРНОЇ СИСТЕМИ ЧИСЛЕННЯ

С.О. Мартиненко, В.А. Краснобаєв

На основі принципів реалізації модульних операція в теорії чисел, запропоновано метод піднесення чисел до квадрату за модулем, на основі якого розроблені пристрої для його реалізації.

Ключові слова: модулярна система числення, модульні операції, піднесення до квадрату.

METHOD OF NUMBERS SQUARED ON MODULE OF M MODULYAR NUMBER SYSTEMS

S.O. Martynenko, V.A. Krasnobayev

On the basis of principles of realization module operation in the theory of numbers the method of erection of numbers is offered in a square on the module, on the basis of which devices are developed for its realization.

Keywords: module number system, module operations, involution.

Мартыненко Сергей Олегович – аспирант кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенка, г. Харьков, Украина.

Краснобаев Виктор Анатольевич – д-р техн. наук, профессор, профессор кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенка, г. Харьков, Украина.