lecturer at the Department of Information Technology of the O.S. Popov Odessa National Academy of Telecommunications.

Задерейко Олександр Владиславович, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія».
E-mail: zadereyko@onua.edu.ua.

Orcid ID: 0000-0003-0497-9861.
Задерейко Александр Владиславович, кандидат технических наук, доцент, доцент кафедры информационных технологий Национального университета «Одесская юридическая академия».
Zadereyko Olexander, Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Information Technologies of the National University "Odessa Law Academy".

DOI: 10.18372/2410-7840.23.15433
УДК 004.81:004.056.5

ПРИСТРІЙ ДЛЯ ПРИВЕДЕННЯ ЧИСЕЛ ЗА МОДУЛЕМ З АНАЛІЗОМ ЧОТИРЬОХ РОЗРЯДІВ ТАКОГО ЧИСЛА ЗА КРОК

Сахибай Тинимбаєв, Сергій Гнатюк, Рат Бердибаєв, Юлія Поліщук, Юлія Бурмак

Сучасна криптографія з відкритим ключем (асиметрична криптографія) дає можливість не лише шифрувати дані, але й вирішувати деякі актуальні проблеми симетричної криптографії – зокрема, проблему розподілу секретних ключів. Проте, алгоритми асиметричної криптографії є досить повільними і ресурсоємними, через що потребують новітніх підходів до підвищення швидкодії та оптимізації їх реалізації на різних платформах. Авторами у статті розглядається питання підвищення швидкодії асиметричних алгоритмів криптографії і пропонується схематичне рішення (пристрій) приведення числа за модулем як одного з методів реалізації приведення цілих чисел за модулем. Відомо, що такі операції, як множення, піднесення до квадрату і приведення за модулем впливають на швидкодію апаратних пристроїв криптографії. Особливо, операція приведення за модулем є найскладнішою і громіздкою в аспекті реалізації, що потребує особливої уваги вчених і дослідників до розробки алгоритмів і апаратних рішень для цієї проблеми. Таким чином, в цій статті авторами пропонується розробка і дослідження пристрою приведення чисел за модулем з аналізом чотирьох розрядів за крок. Розроблений пристрій був верифікований шляхом перевірки створеного алгоритму опису поведінкової моделі на мові Verilog HDL за допомогою часових діаграм. Тестування показало коректність алгоритму поведінкової моделі, що підтвердило ефективність розробленого пристрою приведення чисел за модулем з аналізом чотирьох розрядів такого числа за крок, а також можливість його використання для криптографічних застосувань.
Ключові слова: *асиметрична криптграфія, арифметичні операції, приведення чисел за модулем, схематичне рішення, алгоритм, швидкодія.*

ВСТУП

Сьогодні криптографічні методи і засоби використовуються для забезпечення конфіденційності і цілісності даних у різних галузях, операційних системах і програмних застосунках [1-6]. Криптографія з відкритим ключем дає можливість не лише шифрувати дані, але й вирішувати деякі актуальні проблеми симетричної криптографії – зокрема, проблему розподілу секретних ключів. Проте, алгоритми асиметричної криптографії є досить повільними і ресурсоємними, через що потребують новітніх підходів до підвищення швидкодії та оптимізації [5-9].

АНАЛІЗ ДОСЛІДЖЕНЬ І ПОСТАНОВКА ЗАВДАННЯ

Авторами розглядається питання підвищення швидкодії асиметричних алгоритмів криптографії і пропонується схематичне рішення приведення числа за модулем як одного з методів реалізації приведення цілих чисел за модулем.

Відомо, що такі операції, як множення, піднесення до квадрату і приведення за модулем впливають на швидкодію апаратних пристроїв криптографії [9-12]. Особливо, операція приведення за модулем є найскладнішою і громіздкою в аспекті реалізації, що потребує особливої уваги вчених і дослідників до розробки алгоритмів і апаратних рішень для цієї проблеми [2, 6, 8, 13-25].

З огляду на зазначене, **метою** цієї роботи є розробка і дослідження пристрою приведення

чисел за модулем з аналізом чотирьох розрядів за крок.

Прототипом для приведення числа за модулем є пристрій [26], який містить блок формування кратних модулю P, де формуються значення $P, \bar{P}, 2P, 2\bar{P}, \dots, 7P, 7\bar{P},$ регістр для зберігання 2N- розрядного числа A, N/3 формувачів часткових залишків (ФЧЗ) 8.1÷8.N/3, елемент затримки.

Інформаційні виходи блоку формування кратних P пов'язані з інформаційними входами всіх ФЧЗ 8.1÷8.N/3 для передачі значень я $P, \bar{P}, 2P, 2\bar{P}, \dots, 7P, 7\bar{P}$.

Інформаційні виходи регістра числа A пов'язані з входами всіх ФЧЗ 8.1 ÷8.N/3 для передачі відповідних трьох бітів числа A.

Спочатку залишок R_0 визначається N старшими бітами 2N-розрядного числа A. Зсунутий на три розряди вліво залишок R0 з регістра 5, є числом $A_1 = (8R_0 + a_{n-1}a_{n-2}a_{n-3})$. ФЧЗ 8.1 визначає залишок R_1 за модулем P від числа A_1. Формування числа A_i (i=1÷N/3), яке подається на ФЧЗ 8.i для визначення залишку R_i за модулем P, здійснюється аналогічно.

Отриманий залишок R_{i-1} з виходу ФЧЗ 8.i-1 зсувається вліво на три біта в сторону старших розрядів і до нього приєднуються чергові три молодших біта числа A, які слідують за трьома бітами, використаними на попередньому кроці для формування A_{i-1}:

$$A_i = L(3)R_{i-1} + a_{n-2i+1}a_{n-2i}a_{n-2i-1} = 8R_{i-1} + a_{n-2i+1}a_{n-2i}a_{n-2i-1}.$$

Наприкінці на входи ФЧЗ 8.N/3 подаються біти a_2, a_1 и a_0 числа A і частковий залишок 8RN/3-1 з виходів ФЧЗ 8.N/3-1. На виходах ФЧЗ 8.N/3 формується кінцевий результат $R_{N/3}$=R.

ОСНОВНА ЧАСТИНА ДОСЛІДЖЕННЯ

Подальше підвищення швидкодії вищевказаного пристрою шляхом введення до складу ФЧО семи схем порівняння і блоків схем І і АБО. Входи ФЧЗі з'єднані з виходами блоку формування кратних модуля P, з яких подаються прямі і зворотні коди модулів $P, 2P, \dots, 15P$ і $\bar{P}, \overline{2P}, \dots, \overline{15P}$. Значення часткового залишку з виходів $ФЧЗ_{i-1}$ із зсувом на чотири розряди в сторону старших розрядів з приєднанням наступних чотирьох розрядів числа, що приводиться, подається на ліві входи суматора і схем порівняння ФЧОі, де одночасно порівнюються зі значенням кратних модуля $P, 2P, \dots, 15P$.

За результатами порівняння виробляються керуючі сигнали, які комутують значення одного з кратних модуля $\bar{P}, \overline{2P}, \dots, \overline{15P}$ на праві входи суматора, формуючи на виходах суматора залишку R_i.

На рис. 1 представлена схема пристрою для переведення чисел за модулем. Пристрій містить блок 4 формування кратних модуля P, в якому виробляються значення $P, 2P, \dots, 15P$ і $\bar{P}, \overline{2P}, \dots, \overline{15P}$, регістр 5 для зберігання 2N-розрядної числа A, формувачі часткових залишків ФЧЗ 8.1÷8.N/4, елемент затримки 6.

Інформаційні виходи блоку 4 формування кратних модуля P пов'язані з інформаційними входами всіх ФЧЗ 8.1÷8.N/4 для передачі значення P÷15P и $\bar{P}$÷15$\bar{P}$. Інформаційні виходи регістра 5 числа A пов'язані з входами всіх ФЧЗ 8.1 ÷ 8.N/4 для передачі відповідних чотирьох бітів числа A.

Залишок R_0 визначається N старшими бітами 2N-розрядного числа A. Зсунутий на чотири розряди вліво залишок R_0 з регістра 5, є числом $A_i = (16R_0 + a_{n-1}a_{n-2}a_{n-3})$. ФЧЗ 8.1 визначає залишок R_1 за модулем P від числа A_1.

Формування числа A_i=(i=1÷N/4), яке подається на ФЧЗ 8.i, для визначення залишку R_i за модулем P, здійснюється аналогічно.

Отриманий залишок R_{i-1}, виходу ФЧЗ 8.i-1 зсувається вліво на чотири біта в сторону старших розрядів і до нього приєднуються чергові чотири молодших біта числа A, які слідують за чотирма бітами, використаними на попередньому кроці для формування A_{i-1}.

Тоді:

$$A_i = L(4)R_{i-1} + a_{n-2i+1}a_{n-2i}a_{n-2i-1}a_{n-2i-2} = 16R_{i-1} + a_{n-2i+1}a_{n-2i}a_{n-2i-1}a_{n-2i-2}.$$

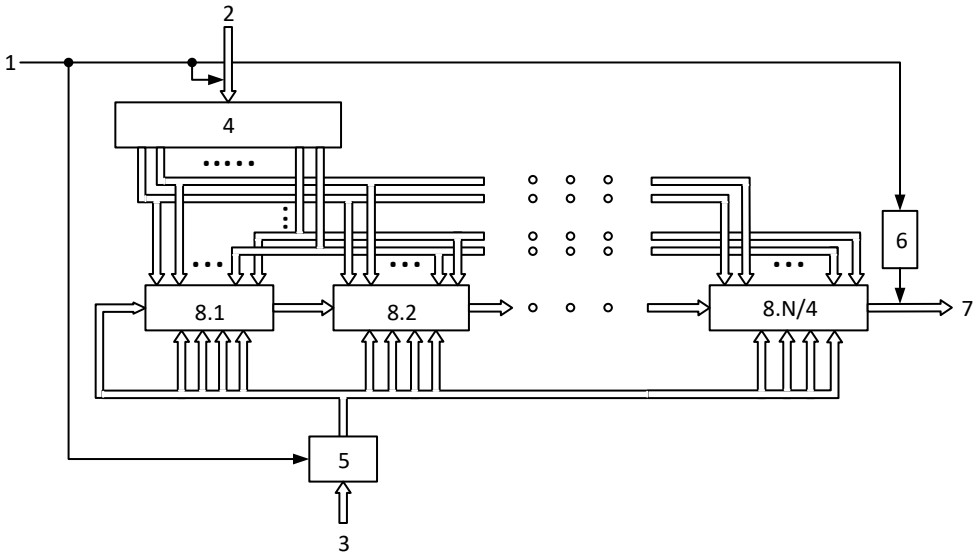

Рис. 1 Пристрій приведення числа за модулем

У кінцевому підсумку на входи ФЧО 8.N/4 з регістра 5 подаються біти a_3, a_2, a_1, a_0 числа А і частковий залишок 16RN/4-1 з виходів ФЧЗ 8.N/4-1. На виходах ФЧЗ 8.N/4 формується кінцевий результат $R_{N/4}$=R.

Розглянемо роботу пристрою приведення 2N-розрядного числа А за N-разрядним модулем Р. За сигналом «Пуск», який подається на вхід 1, значення Р з входу 2 приймається в блок формування 4 кратних модулю Р. Значення числа А з входу 3 приймається в регістр 5. Значення $P, \bar{P}, 2P, \overline{2P}, \ldots, 15P, \overline{15P}$ з виходів блоку 4 подаються на входи всіх ФЧЗ 8.1÷8.N/4.

Одночасно N старших бітів числа А (тобто R_0) з виходів регістру 5 числа А із зсувом на чотири розряду в сторону старших розрядів подаються на входи ФЧЗ 8.1. При цьому до молодших розрядів здвинутого коду R0 з регістра 5 приєднуються біти $a_{n-1}a_{n-2}a_{n-3}a_{n-4}$ числа А, утворюючи число A_1. ФЧЗ 8.1 визначає залишок R_1.

Далі значення R_1 зі здвигом на чотири розряду в сторону старших розрядів, а також біти $a_{n-4}a_{n-5}a_{n-6}a_{n-7}$ числа А з регістра 5 утворюють A_2 і подаються на входи ФЧЗ 8.2, формуючи частковий залишок R_2 і т.д. На заключному етапі частковий залишок RN/4-1 з виходів попереднього ФЧЗ 8. RN/4-1 зі зрушенням на чотири розряди в сторону старших розрядів і біти a_3, a_2, a_1, a_0 числа А з регістра 5 надходять на входи ФЧО 8.N / 4 і на його виходах формується залишок $R_{N/4}$.

Сигналом «Кінець операцій», який формується на виході елемента затримки 6, залишок $R_{N/4}$ подається на вихід пристрою 7. Час формування результату $T_{фр}$ визначається сумарним часом проходження сигналу через ФЧЗ, тобто $T_{фр}=N/4T_{ФЧЗ}$. Основним блоком пристрою для приведення числа за модулем є ФЧЗ. На рис. 2 представлена функціональна схема $ФЧО_i$, яка складається з двійкового суматора СМ, семи схем порівнянь СС-1÷СС-7, блоків схем І0÷І30, схем І31-І35, блоків схем АБО1÷АБО5 і схеми АБО6.

Значення попереднього залишку R_{i-1} зсунутого вліво на чотири розряди в сторону старших розрядів, з приєднанням до нього чергових чотири молодші біти числа А, визначає значення A_i:

$$A_i = 16R_{i-1} + a_{n-2i+1}a_{n-2i}a_{n-2i-1}a_{n-2i-2}.$$

Значення A_i подається на ліві входи суматора і на ліві входи схем СС-1 ÷ СС-7, де виконується порівняння з кратними модуля Р. Робота схем порівняння СС-1 ÷ СС-4 залежить від результату порівняння A_i з кодами 5Р, 9Р, 13Р на схемах СС-5, СС-6, СС-7 відповідно. Залежно від цього результату схемою СС-1 значення A_i порівнюється з кодами Р або 5К, або 9Р, або 13р; схемою СС-2 Аі порівнюється з кодами 2Р або 6Р, або 10Р, чи 14Р; схемою СС-3 A_i порівнюється з кодами 3Р або 7Р, або 11р, або 15Р; схемою СС-4 A_i порівнюється з кодами 4Р або 8Р, або 12Р, або 14Р.

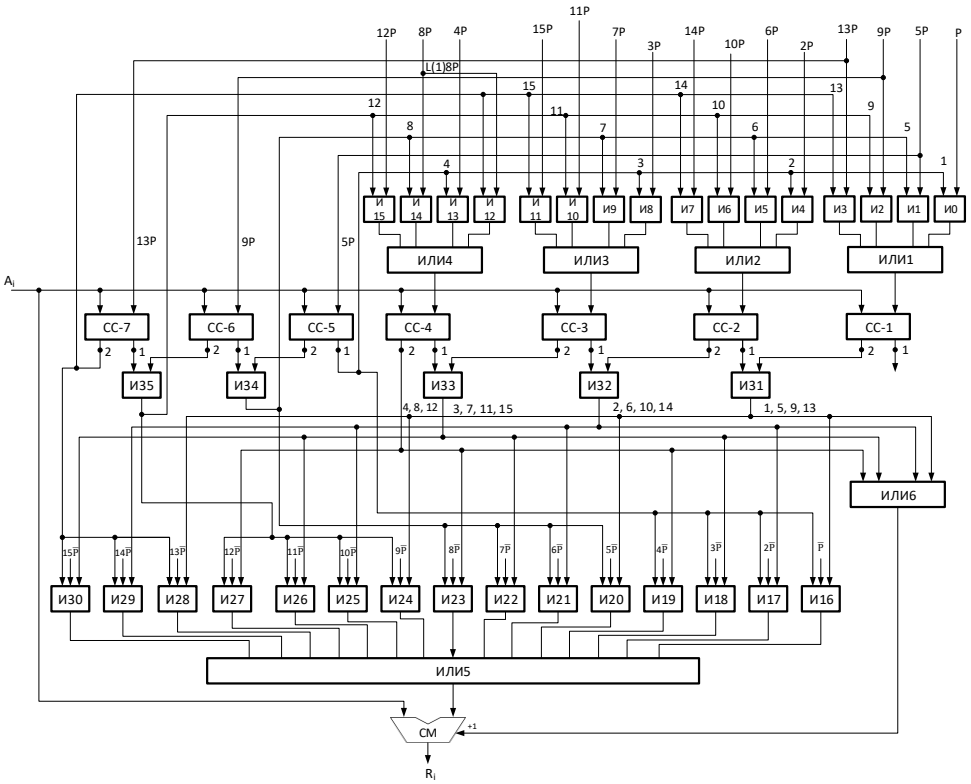

Рис. 2 Функціональна схема формувача часткового залишку (ФЧЗ)

Якщо в результаті порівняння 5Р з A_i на схемі СС-5 має місце співвідношення $A_i<5P$, то на виході 1 СС-5 виробляється сигнал «1», який комутує значення кодів Р, 2Р, 3Р, 4Р блоками схем І0, І4, І8 і І13 на праві входи відповідних схем порівняння СС-1, СС-2, СС-3 і СС-4, де вони порівнюються із значенням A_i. Одиничний сигнал з виходу 1 СС-5 також подається на керуючі входи блоків схем І16, І17, та І18, І19 для дозволу проходження в подальшому на суматор СМ кодів $\overline{P}$ **чи** $\overline{2P}$**, чи,** $\overline{3P}$ **чи** $\overline{4P}$, які подаються на інформаційні входи схем І16 ÷ І19, відповідно.

Якщо в результаті порівняння 9Р з A_i на схемі СС-6 і порівняння 5Р з A_i на схемі порівняння СС-5 має місце співвідношення $9P>A_i\geq5P$, то на виході 2 схеми СС-5 і на виході 1 схеми СС-6 виробляються сигнали «1», які подаються на входи схеми І34. В результаті на виході схеми І34 виробляється сигнал «1», який комутує значення кодів 5Р, 6Р, 7Р і 8Р блоками схем І1, І5, І9, та І14 на праві входи відповідних схем порівняння СС-1, СС-2, СС-3, СС-4, де вони порівнюються з A_i. Одиничний сигнал з виходу схеми І34 також подається на керуючі входи блоків схем І20, І21, І22, І23 для дозволу проходження в подальшому на суматор СМ кодів $\overline{5P}$ **чи** $\overline{6P}$**, чи,** $\overline{7P}$ **чи** $\overline{8P}$, які подаються на інформаційні входи схем І20 ÷ І23, відповідно.

Якщо в результаті порівняння 9Р з A_i на схемі СС-6 і 13Р з A_i на схемі порівняння СС-7 має місце співвідношення $13P>A_i\geq9P$, то на виході 2 СС-6 і на виході 1 схеми СС-7 виробляються сигнали «1 », які подаються на входи схеми І35. В результаті на виході схеми І35 виробляється сигнал «1», який комутує значення кодів 9Р, 10Р, 11Р і 12Р блоками схем І2, І6, І10 і І15 на праві входи відповідних схем порівняння СС-1, СС-2, СС-3 і СС-4, де вони порівнюються з A_i. Одиничний сигнал з виходу схеми І35 також подається на керуючі входи блоків схем І24, І25, І26, І27 для дозволу проходження в подальшому на суматор СМ кодів $\overline{9P}$ **чи** $\overline{10P}$**, чи,** $\overline{11P}$ **чи** $\overline{12P}$, які подаються на інформаційні входи схем І24 ÷ І27, відповідно.

При порівнянні A_i з 13Р на схемі СС-7, якщо має місце співвідношення $A_i\geq13P$, то на її виході 2 виробляється сигнал «1», який комутує значення кодів 13Р, 14Р, 15Р, 16Р (утворюється зсувом вліво на один розряд значення 8Р) блоками І3, І7, І11, І12 через відповідні блоки схем АБО1, АБО 2, АБО 3, АБО4 на праві входи відповідних схем

порівняння СС-1, СС-2, СС-3 і СС-4, де вони порівнюються з A_i.

Одиничний сигнал з виходу 2 СС-7 також подається на керуючі входи блоків схем І28, І29, І30 для дозволу проходження в подальшому на суматор СМ кодів $\overline{13P}$ чи $\overline{14P}$, чи, $\overline{15P}$, які подаються на інформаційні входи схем І28 ÷ І30, відповідно .

При порівнянні A_i з Р на схемі СС-1, якщо A_i <Р жодна зі схем І16-І35 не спрацює. Значення A_i, подане на лівий вхід суматора СМ, підсумовується з нулем і на виході суматора формується $R_i=A_i$.

При порівнянні Р з A_i на схемі СС-1 і коду 2Р з A_i на схемі СС-2, якщо значення коду 2Р>A_i≥Р, то на виході схеми І31 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І16, що призводить до виконання на суматорі СМ операції $R_i = A_i + \bar{P} + 1$.

При порівнянні коду 2Р з A_i на схемі СС-2 і коду 3Р з A_i на схемі СС-3, якщо виконується умова 3Р> A_i ≥2Р, то вихід схеми І32 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І17, що призводить до виконання на суматорі СМ операції $R_i = A_i + \overline{2P} + 1$.

При порівнянні коду 3Р з A_i на схемі СС-3 і коду 4Р з A_i на схемі СС-4, якщо виконується умова 4Р> A_i ≥3Р, то на виході схеми І33 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І18, що призводить до виконання на суматорі СМ відповідної операції $R_i = A_i + \overline{3P} + 1$.

При порівнянні коду 4Р з A_i на схемі СС-4, якщо виконується умова A_i ≥4Р, то на його 2 виході виробляється одиничний сигнал, який подається на вхід схеми АБО6 і на третій вхід блоку схем І19, що призводить до виконання на суматорі СМ операції $R_i = A_i + \overline{4P} + 1$.

При порівнянні коду 5Р з A_i на схемі СС-1 і коду 6Р з A_i на схемі СС-2 якщо виконується умова 6Р>A_i ≥5Р, то на виході схеми І31 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І20, що призводить до виконання на суматорі СМ відповідної операції $R_i = A_i + \overline{5P} + 1$.

При порівнянні коду 6Р з A_i на схемі СС-2 і коду 7Р з A_i на схемі СС-3, якщо виконується умова 7Р> Аі ≥6Р, то на виході схеми І32 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І21, що призводить до виконання на суматорі СМ відповідної операцій $R_i = A_i + \overline{6P} + 1$.

При порівнянні коду 7Р з A_i на схемі СС-3 і коду 8Р з A_i на схемі СС-4, якщо виконується умова 8Р>A_i ≥7Р, то на виході схеми І33 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І22, що призводить до виконання на суматорі СМ операції $R_i = A_i + \overline{7P} + 1$.

При порівнянь коду 8Р з A_i на схемі СС-4, якщо A_i≥8Р, то на виході 2 СС-4 формується одиничний сигнал, який подається на вхід схеми АБО6 і на третій вхід блоку схем І23, що призводить до виконання на суматорі СМ операції $R_i = A_i + \overline{8P} + 1$.

При порівнянь коду 9Р з A_i на схемі СС-1 і коду 10Р з A_i на схемі СС-2, якщо виконується умова 10Р>A_i ≥9Р, то на виході схеми І31 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І24, що призводить до виконання на суматорі СМ операції $R_i = A_i + \overline{9P} + 1$. При порівнянні коду 10Р з A_i на схемі СС-2 і коду 11Р з A_i на схемі СС-3, якщо виконується умова 12Р>A_i ≥11Р, то на виході схеми І32 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І25, що призводить до виконання на суматорі СМ операції $R_i = A_i + \overline{10P} + 1$.

При порівнянні коду 11Р з A_i на схемі СС-3 і коду 12Р з A_i на схемі СС-4, якщо виконується умова 12Р>A_i ≥11Р, то на виході схеми І33 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І26, що призводить до виконання на суматорі СМ відповідної операції: $R_i = A_i + \overline{11P} + 1$.

При порівнянні коду 12Р з A_i на схемі СС-4, якщо A_i≥12Р, то на виході 2 СС-4 формується одиничний сигнал, який подається на вхід схеми АБО6 і на третій вхід блоку схем І27, що призво-

дить до виконання на суматорі СМ відповідної операції $R_i = A_i + \overline{12P} + 1$.

При порівнянні коду 13P з A_i на схемі СС-1 і коду 14P з A_i на схемі СС-2, якщо виконується умова $14P > A_i \geq 13P$, то на виході схеми І31 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І28, що призводить до виконання на суматорі СМ операції $R_i = A_i + \overline{13P} + 1$.

При порівнянь коду 14P з A_i на схемі СС-2 і коду 15P з A_i на схемі СС-3, якщо виконується умова $15P > A_i \geq 14P$, то на виході схеми І32 формується сигнал «1», який подається на вхід схеми АБО6 і на третій вхід блоку схем І29, що призводить до виконання на суматорі СМ операцій $R_i = A_i + \overline{14P} + 1$.

При порівнянь коду 15P з A_i на схемі СС-3 і коду 16P з A_i на схемі СС-4, якщо виконується умова $16P > A_i > 15P$, то на виході схеми І33 формується одиничний сигнал, який подається на вхід схеми АБО6 і на третій вхід блоку схем І30, що призводить до виконання на суматорі СМ операцій $RR_i = A_i + \overline{15P} + 1$.

Нижче розглядається приклад приведення 2N-розрядного числа A за N-разрядним модулем P.

Нехай

$$A = 35035_{10} = \begin{cases} a_{15}a_{14}a_{13}a_{12}a_{11}a_{10}a_9a_8a_7a_6a_5a_4a_3a_2a_1a_0 \\ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1 \end{cases}.$$

Старші 8 бітів двійкового числа A визначають значення $R_0 = 10001000_2 = 136_{10}$.

$$N=8,\ N/4=2;$$

$$P = 187_{10} = 10111011_2; 2P = 374_{10}; 3P = 561_{10}; 4P = 748_{10}; 5P = 935_{10}; 6P = 1122_{10}; 7P = 1309_{10}; 8P = 1496_{10}; 9P = 1683_{10}; 10P = 1870_{10}; 11P = 2057_{10}; 12P = 2244_{10}; 13P = 2431_{10}; 14P = 2618_{10}; 15P = 2805_{10}.$$

До здинутого вліво на чотири розряду залишку R_0, приєднуючи наступні біти $a_7a_6a_5a_4$ числа A, отримаємо:

$$A_i = L(4)R_0 + (a_7a_6a_5a_4) = 16R_0 + (1101_2) = (2176_{10}) + (13_{10}) = 2189_{10}.$$

Для наочності всі обчислення щодо визначення залишку R=AmodP наведені в табл.1 в десятковій системі числення.

Перевірка: R=AmodP=35035mod187=66.

Експериментальне дослідження

Перевірка створеного алгоритму опису поведінкової моделі на мові Verilog HDL була виконана за допомогою часових діаграм для значень числа A і модуля P (рис. 3). Тестування показало коректність алгоритму поведінкової моделі.

Таблиця 1

Порядок обчислення R=AmodP

1-етап ФЧЗ.1	$A_1 = L(4)R_0 + (a_7a_6a_5a_4) = 2176_{10} + (13_{10}) = 2189_{10}$ Так як $2057_{10} < 2189_{10} < 2244_{10}$, то має місце співвідношення $11P < A_1 < 12P$. Отже, виконується операція: $R_1 = 2189_{10} - 11P = 2189_{10} - 2057_{10} = 132_{10}$
2-етап ФЧЗ.2	$A_2 = L(4)R_1 + (a_3a_2a_1a_0) = 2112_{10} + (11_{10}) = 2123_{10}$ Так як $2057_{10} < 2123_{10} < 2244_{10}$, то має місце співвідношення $11P < A_2 < 12P$. Отже, виконується операція: $R_1 = 2123_{10} - 2057_{10} = 66_{10}$

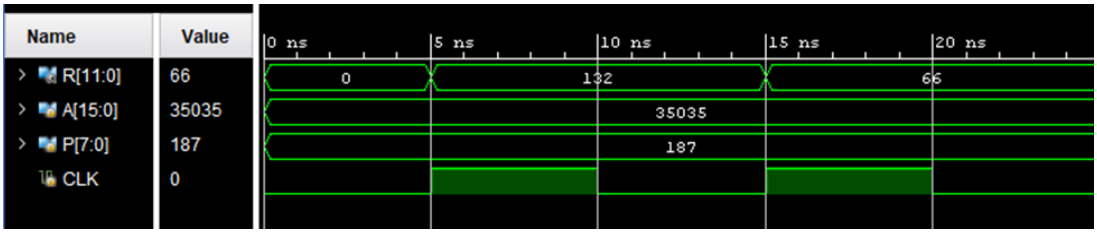

Рис. 3 Часові діаграми при значенні числа A = 35035 і модуля P = 187

ВИСНОВКИ

У статті розглядалося питання підвищення швидкодії асиметричних алгоритмів криптографії і запропоновано схематичне рішення (пристрій) приведення числа за модулем як одного з методів реалізації приведення цілих чисел за модулем. Авторами пропонується розробка і дослідження пристрою приведення чисел за модулем з аналізом чотирьох розрядів за крок. Розроблений пристрій був верифікований шляхом перевірки створеного алгоритму опису поведінкової моделі на мові Verilog HDL за допомогою часових діаграм. Тестування показало коректність алгоритму поведінкової моделі, що підтвердило ефективність розробленого пристрою приведення чисел за модулем з аналізом чотирьох розрядів такого числа за крок, а також можливість його використання для криптографічних застосувань.

ЛІТЕРАТУРА

[1] Hars L., Joye M., Quisquater J. J. (eds). Long Modular Multiplication for Cryptographic Applications // Cryptographic Hardware and Embedded Systems CHES 2004. *Lecture Notes in Computer Science, 2004*. V. 3156. Springer, Berlin, Heidelberg, 2004. – 15p.

[2] Петренко В.И., Сидорчук А.В., Кузьминов Ж.В. *Устройство для формирования остатка по произвольному модулю* // Патент РФ 2368942 С2 (2009).

[3] Панкратова И.А. *Теоретико-числовые методы криптографии*. - Томский государственный университет, 2009. - 120 с.

[4] Захаров В.М., Столов Е.Л., Шалагин С.В. *Устройство для формирования остатка по заданному модулю* // Патент РФ 2421781 С2 (2011).

[5] Копутов В.В., Петренко В.И., Сидорчук А.В. *Устройство для формирования остатка по произвольному модулю от числа* // Патент РФ 2445730 С2 (2012).

[6] Скрябин И., Сахин Ю.Х. *Операции поддержки алгоритмов шифрования с открытым ключом и их реализация в микропроцессоре*. – Эльбрус, 2013 / [Электронный ресурс]: http://www.myshared.ru/slide/213088.

[7] Pisek E., Henige T. M. *Method and apparatus for e cient modulo multiplication* // Patent US 8417756 B2 (2013).

[8] Lambert R. J. Method and apparatus for modulus reduction // Patent US 08862651 B2. (2014).

[9] Айтхожаева Е.Ж., Тынымбаев С.Т. *Аспекты аппаратного приведения по модулю в асимметричной криптографии* // Вестник НАН РК, 2014, - N 5 (375), С. 88-93.

[10] Bockes M., Pulkus J. *Method for arbitrary-precision division or modular reduction* // Patent US 9042543 B2 (2015).

[11] Yu H., Bai G., Hao H., Wang J., Yap C. (eds). E cient Modular Reduction Algorithm Without Correction Phase // Frontiers in Algorithmics. FAW 2015. Lecture Notes in Computer Science, 2015. V. 9130. Springer, Cham, 2015. – 340 p.

[12] Kovtun M., Kovtun V. *Обзор и классификация алгоритмов деления и приведения по модулю больших целых чисел для криптографических приложений* / Kompaniya Sayfer. 2017. [Electron. resource]: http://docplayer.ru/30671408-Obzor-i-klassifikaciya-algoritmov-deleniya-iprivedeniya-po-modulyu-bolshih-celyh-chisel-dlya-criptograficheskih-prilozheniy. html.

[13] А.с. 1422. *Устройство быстрого приведения чисел по модулю* / Тынымбаев С., Айтхожаева Е.Ж., Әділбекқызы С. Опубл. 11.05.2018 г. – 1с.15.

[14] Тынымбаев С.Т., Бердибаев Р.Ш., Омар Т., Шайкулова А.А., Магауин Б. Быстродействующие устройства приведения числа по модулю // *Матер. IV Междунар. Азиатской школы-семинара «Проблемы оптимизации сложных систем»*. – Кыргызская Республика, оз. Иссыккуль, пансионат «Отель Евразия». - Ч2, 20-31 июля 2018. – С. 273-279.

[15] *А.с. 2752. Устройство быстрого приведения чисел по модулю на базе делителя с блокировкой отрицательных остатков* / Тынымбаев С, Бердибаев Р.Ш., Омар Т., Магауин Б.А. Опубл. 24.08.2018 г. – 1с.

[16] *А.с. 2753. Устройство быстрого приведения числа по модулю на сумматорах* / Тынымбаев С., Бердибаев Р.Ш., Омар Т., Әділбекқызы С. Опубл. 24.08.2018 г. – 1с.

[17] *А.с. 2754. Конвейеризированная схема приведения модулю* /Тынымбаев С.Т., Бердибаев Р.Ш., Омар Т., Нурлыбаев А., Шайкулова А.А. Опубл. 24.08.2018 г. – 1с.

[18] Tynymbayev S., Gnatyuk S.A., Aitkhozhayeva Y. Zh., Berdibayev R.Sh., Namazbayev T.A. Modular reduction based on the divider by blocking negative remainders // *News of the National Academy of Sciences of the Republic of Kazakhstan. Series of Geology and Technical Sciences*. - №2 (434). – Алматы, Наука, 2019. - С. 238-248.

[19] Әділбеккызы С., Айтхожаева Е.Ж., Тынымбаев С. Моделирование формирователя частичных остатков устройства приведения по модулю. // *Евразийский Союз Ученых (ЕСУ)*, № 6 (63), 2 часть (2019). – Москва, 2019. – С. 47-51.

[20] *Патент на изобретение 33182 Республики Казахстан от 29.07.2019 г. Устройство для приведения чисел по модулю* / Тынымбаев С., Айтхожаева Е.Ж., Мамырбаев О.Ж., Әділбекқызы С.; pfzd/ 11.02.2019. – 1 с.

[21] Tynymbayev S., Gnatyuk S.A., Aitkhozhayeva Y. Zh., Berdibayev R.Sh., Namazbayev T.A. Tetyana Okhrimenko T. Development of Modular Reduction Based on the Divider by Blocking Negative Remainders for Critical Cryptographic Application // *2019 IEEE 2-nd Ukraine Conference on Electrical and Computer Engineering*. - Lviv, Ukraine, July 2-6, 2019. - С. 809-812.

[22] S. Tynymbayev, R. Sh. Berdibayev, T. Omar, S. A. Gnatyuk, T. A. Namazbayev, S. Adilbekkyzy. Devices for multiplying modulo numbers with analysis of the lower bits of the multiplier. // *Bulletin of National Academy of Sciences of the Republic of Kazakhstan*, № 4 . - Алматы: Наука, 2019. – С. 38-45.

[23] S. Tynymbayev, R. Berdibayev, T. Omar, Y. Aitkhozhayeva, A. Shaikulova and S. Adilbekkyzy. High-speed devices for modular reduction with minimal hardware costs // *Cogent Engineering (2019)*, 6: 169 7555.

[24] С. Тынымбаев, Е.Ж. Айтхожаева, С. Әділбекқызы, Р. Ш. Бердибаев. Разработка и моделирование принципиальной схемы устройства приведения по модулю // *Журнал «Проблемы информатики»*, - ИВМиМГ СО РАН, ИИВТ КН МОН РК, -2019. - № 4. - С.42-52.

[25] S. Tynymbayev, T. R. Berdibayev, Omar, S. Gnatyuk, T. Namazbayev, S. Adilbekkyzy. Devices for Modular Multiplication of Numbers with Analysis of Two Least Significant Bits of the Multiplier // *1st International conference on cyber hygiene & conflict management in global information networks,* - Kyiv and Lviv, Ukraine during November 29-30, 2019, http://ceur-ws.org/Vol-2654/paper59.pdf.

[26] *Пат. 34255 Республика Казахстан. Устройство для приведения чисел по модулю с анализом 3-х разрядов приводимого числа за шаг* / Тынымбаев С., Айтхожаева Е.Ж. Мамырбаев О, Әділбекқызы С.; опубл. 03.04.2020г. – 1с.

УСТРОЙСТВО ПРИВЕДЕНИЯ ЧИСЕЛ ПО МОДУЛЮ С АНАЛИЗОМ ЧЕТЫРЕХ РАЗРЯДОВ ПРИВОДИМОГО ЧИСЛА ЗА ШАГ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЙ

Современная криптография с открытым ключом (асимметричная криптография) дает возможность не только шифровать данные, но и решать некоторые актуальные проблемы симметричной криптографии - в частности, проблему распределения секретных ключей. Однако, алгоритмы асимметричной криптографии достаточно медленные и ресурсоемкие, по этому требуются новые подходы к повышению быстродействия и оптимизации их реализации на различных платформах. Авторами в статье рассматривается вопрос повышения быстродействия алгоритмов асимметричной криптографии и предлагается схематическое решение (устройство) приведение числа по модулю как одного из методов реализации сведения целых чисел по модулю. Известно, что такие операции, как умножение, возведение в квадрат и приведение по модулю влияют на быстродействие аппаратных устройств криптографии. Особенно, операция приведения по модулю является сложной и громоздкой в аспекте реализации, что требует особого внимания ученых и исследователей к разработке алгоритмов и аппаратных решений для этой проблемы. Таким образом, а этой статье авторами предлагается разработка и исследование устройства приведения чисел с модулем с анализом четырех разрядов за шаг. Разработанное устройство было верифицировано путем проверки созданного алгоритма описания поведенческой модели на языке Verilog HDL с помощью временных диаграмм. Тестирование показало корректность алгоритма поведенческой модели, что подтвердило эффективность разработанного устройства приведения чисел с модулем с анализом четырех разрядов такого числа за шаг, а также возможность его использования для криптографических приложений.

Ключевые слова: асимметричная криптгрфия, арифметические операции, приведение чисел по модулю, схематическое решение, алгоритм, быстродействие.

DEVICE FOR REDUCING NUMBERS MODULO WITH ANALYSIS OF FOUR-BITS OF SUCH NUMBER PER STEP FOR CRYPTOGRAPHICAL APPLICATIONS

Today a lot of cyberattacks are directed on the data and other resources of information and communication systems. Cryptography is used to provide confidentiality and integrity of various types of the data (personal, confidentional, sensitive). Symmetric algorithms (block and stream) have high speed parameters to provide data security and privacy in communicational channels. But symmetric ciphers have some problems and disadvantages that must be solved for effective functionning. Modern public key cryptography (asymmetric cryptography) makes it possible not only to encrypt data, but also to solve some current problems of symmetric cryptography – in particular, the problem of distribution of secret keys. However, asymmetric cryptography algorithms are quite slow and resource-intensive, which is why they require the latest approaches to increase performance and optimize their implementation on different platforms. The authors consider the issue of increasing the speed of asymmetric cryptography algorithms and propose a schematic solution (device) for reducing a number by modulus as one of the methods of implementing the summation of integers by modulus. It is known that operations such as multiplication, squaring and modulation affect the performance of cryptographic hardware devices. In particular, the modular operation is the most complex and cumbersome in terms of implementation, which requires special attention of scientists and researchers to develop algorithms and hardware solutions for this problem. From this position, in the paper authors propose to develop and study a device for reducing numbers modulo with the analysis of four digits per step. The developed device was verified by checking the created algorithm for describing the behavioral model in Verilog HDL using time diagrams. The testing showed the correctness of the algorithm of the behavioral model, which confirmed the effectiveness of the developed device for bringing numbers modulo with the analysis of four digits of such a number per step, as well as the possibility of its use for cryptographic applications.

Keywords: asymmetric cryptography, arithmetic operations, modular number reduction, schematic solution, algorithm, speed.

Сахибай Тинимбайович Тинимбаєв, к.т.н., професор кафедри інформаційних систем та кібербезпеки Алматинського університету енергетики та зв'язку.
E-mail:. s.tynym@gmail.com.
Orcid ID: 0000-0002-9326-9476.
Сахыбай Тынымбаевич Тынымбаев, к.т.н., профессор кафедры информационных систем и кибербезопасности Алматинского университета энергетики и связи.
Sakhybay Tynymbayev, PhD, Professor of Information Systems and Cybersecurity Academic Department, Almaty University of Power Engineering and Telecommunication.

Гнатюк Сергій Олександрович, д.т.н., доцент, заступник декана Факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua.
Orcid ID:0000-0003-4992-0564.
Гнатюк Сергей Александрович,. д.т.н., доцент, заместитель декана Факультета кибербезопасности, компьютерной и программной инженерии Национального авиационного университета.
Sergiy Gnatyuk, DSc, Associate Professor, Vice-Dean of the Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University.

Бердибаєв Рат Шиндалійович, доцент кафедри інформаційних систем та кібербезпеки Алматинського університету енергетики та зв'язку.
E-mail: r.berdybaev@aues.kz.
Orcid ID: 000-0002-8341-9645.
Бердибаев Рат Шиндалиевич, доцент кафедры информационных систем и кибербезопасности Алматинского университета энергетики и связи.
Rat Berdibayev,. PhD, Associate Professor of Information Systems and Cybersecurity Academic Department, Almaty University of Power Engineering and Telecommunication.

Поліщук Юлія Ярославівна, аспірант PhD, Національний авіаційний університет.
E-mail: liya7954@gmail.com.
Orcid ID:. 0000-0002-0686-2328.
Полищук Юлия Ярославовна, аспирант PhD, Национальный авиационный университет.
Yuliia Polishchuk, PhD student, National Aviation University.

Бурмак Юлія Анатоліївна, викладач Київського коледжу зв'язку.
E-mail: kulikovskau@gmail.com.
Orcid ID:. 0000-0002-8090-5058.
Бурмак Юлия Анатолиевна, преподаватель Киевского колледжа связи.
Yuliia Burmak, Lecturer in Kyiv College of Communication.

DOI: 10.18372/2410-7840.23.15434
УДК 004:591.5:612:616-006

КОНЦЕПТУАЛЬНІ ЗАСАДИ ВПРОВАДЖЕННЯ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ МОДЕЛІ КІБЕРЗАХИСТУ УКРАЇНИ

Олександр Потій, Андрій Семенченко, Дмитро Дубов, Олександр Бакалинський, Данило Мялковський

У статті запропоновано концептуальні засади впровадження організаційно – технічної моделі кіберзахисту. Зокрема, визначені її місія, мета, призначення та цілі. Вперше визначені сили та засоби кіберзахисту. Розглянуто архітектуру організаційно-технічної моделі кіберзахисту, яка являє собою структуровану систему, яка складається з трьох інфраструктур кіберзахисту, а саме: організаційно-керуючу інфраструктуру кіберзахисту, як сукупність суб'єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки; технологічну інфраструктуру кіберзахисту, як сукупність сил та засобів кіберзахисту, а також інфраструктури, що забезпечує функціонування сил кіберзахисту, інформаційно-комунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту та базисну інфраструктуру кіберзахисту, як сукупність об'єктів критичної інформаційної інфраструктури, критичних активів, комунікаційних і технологічних систем підприємств, установ та організацій, що віднесені до об'єктів критичної інфраструктури, а також суб'єктів господарювання, громадян України та об'єднань громадян, інших особі, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. Отже, впровадження організаційно-технічної моделі кіберзахисту спрямовано на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів та мінімізацію вразливості комунікаційних систем.

Ключові слова: *національна система кібербезпеки, критична інфраструктура, критична інформаційна інфраструктура, організаційно-технічна модель, кіберзахист.*