УДК 004.056

СТРУКТУРИ СПЕЦІАЛІЗОВАНИХ ПРОЦЕСОРІВ ДЛЯ ГЕШУВАННЯ, СТІЙКОГО ДО ЗАГАЛЬНИХ АТАК

Ю. В. Баришев, к. т. н., ст. викладач; А. О. Зозуля
Вінницький національний технічний університет
yuriy.baryshev@gmail.com

Для функціонування інформаційних технологій періодично необхідно розв'язувати задачі автентифікації даних та користувачів. Для криптографічностійкої автентифікації використовують алгоритми гешування. Однак, більшість криптографічних операцій не природні для використання на сучасних процесорах, прикладом однієї з таких операцій є операція піднесення до степеня за модулем простого числа. Саме тому необхідно розробляти спеціалізовані мікропроцесори, для яких ці операції стануть природніми.

Метою дослідження є збільшення швидкості гешування даних при використанні операцій з теоретично доведеною стійкістю до зламу.

Одним з найбільш використовуваних криптографічних перетворень, злам яких зводиться до задач теоретично доведеної стійкості, є операція піднесення до степеня за допомогою простого числа. Гешування на основі цього перетворення має такий вигляд:

$$h_i \equiv g^{\left(m_i + h_{i-1}\right)} \bmod p,$$

де h – проміжне геш-значення, g – примітивний елемент з модулем p.

Оскільки користувачі вимагають від інформаційних технологій швидкості роботи, тому пропонується розпаралелювати обчислення при гешуванні:

$$\begin{cases} h_i^{(1)} \equiv g^{\left(m_i + h_{i-1}\right)} \bmod p^{(1)}; \\ h_i^{(2)} \equiv g^{\left(m_i + h_{i-1}\right)} \bmod p^{(2)}; \\ \ldots \\ h_i^{(q)} \equiv g^{\left(m_i + h_{i-1}\right)} \bmod p^{(q)}; \\ h_i \equiv \prod_j h_{i-1}^{(j)}, \end{cases}$$

де q – кількість каналів.

Для того, щоб гешування було унікальним для кожного з каналів, тобто кожен канал виконував притаманну лише йому функцію, пропонується гешування такого виду:

$$\begin{cases} h_i^{(1)} \equiv g^{\left(m_i + h_{i-1} + h_{i-1}^{(1)}\right)} \bmod p^{(1)}; \\ h_i^{(2)} \equiv g^{\left(m_i + h_{i-1} + h_{i-1}^{(2)}\right)} \bmod p^{(2)}; \\ \ldots \\ h_i^{(q)} \equiv g^{\left(m_i + h_{i-1} + h_{i-1}^{(q)}\right)} \bmod p^{(q)}; \\ h_i \equiv \prod_j h_{i-1}^{(j)}. \end{cases}$$

Розроблений мікропроцесор передбачає паралельну обробку даних, що дозволяє для досягнення мети використовувати математичні моделі паралельного гешування, які розглянуті вище.

Розроблено загальну схему мікропроцесора (рис. 1), що складається з інтерфейсу (в якості інтерфейсу обрано UART), лічильника, блоку пам’яті, який зберігає поточне значення, блоків піднесення – виконують криптографічне перетворення, блоку множення, який поєднує проміжні геш-значення.

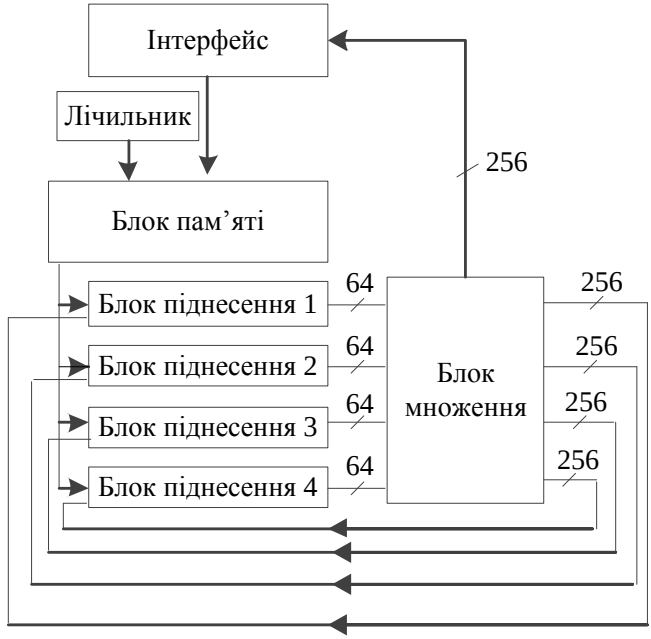

Рисунок 1 – Загальна схема мікропроцесора

Блок піднесення забезпечує необхідний рівень швидкості гешування даних, використовуючи бінарний алгоритм піднесення до степеня. Використання такого методу обумовлюється високою продуктивністю виконання операцією та водночас низькими вимогами до апаратного забезпечення, яке його реалізовуватиме. Схема блоку піднесення наведена на рисунку 2.

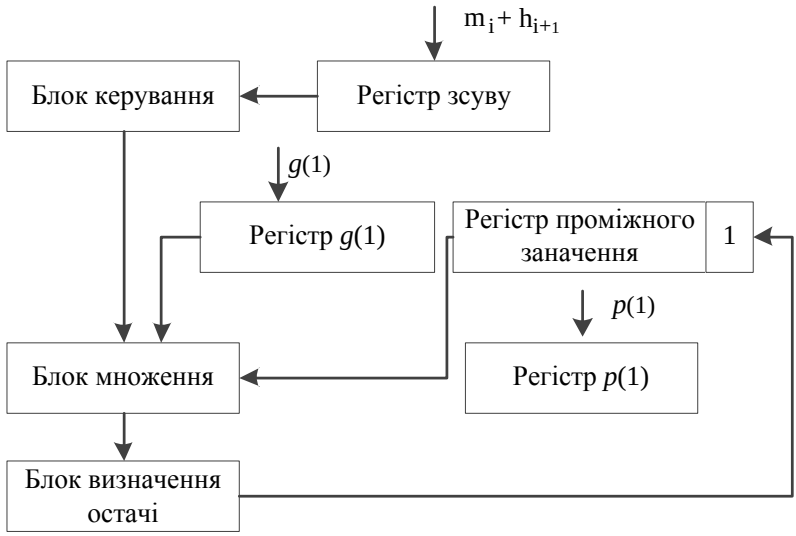

Рисунок 2 – Загальна схема мікропроцесора

На рисунку 2 блок керування та регістр зсуву для першої математичної моделі на кожній ітерації залишається однаковий, для другої – вони будуть унікальними.

Даний процесор було описано мовою VHDL та змодельовано його роботу в середовищі ModelSim. Експерименти показали, що використання спеціалізованого мікропроцесорного пристрою дозволяє отримати виграш продуктивності при гешуванні даних порівняно з програмною моделлю реалізації цього ж методу гешування.