Методи та структури спеціалізованих процесорів для гешування стійкого до загальних атак

Доповідач: магістрант, студент гр. ЗІ-14м Зозуля А. О.
Науковий керівник: к. т. н., доц. Баришев Ю. В.
Кафедра захисту інформації
Вінницький національний технічний університет

Об'єкт – процес криптографічного захисту інформації.

Предмет – апаратні засоби криптографічного захисту інформації.

Мета: збільшити швидкість гешування даних алгоритмом з теоретично доведеною стійкістю, розробивши спеціалізований процесор.

Задачі:

- Проаналізувати загальні атаки;
- Розробити алгоритм гешування даних;
- Розробити методи гешування даних;
- Розробити структуру спеціалізованого пристрою.

Суттєвий внесок у розвиток даної галузі зробили такі вчені як: Бабенко В. Г., Бойко А. О. Корченко О. Г., Лєншина Ю. М., Лужецький В. А., Найеф М. А. А., Рудницький В. М., Бертоні Г., Келсі Дж., Коно Т., Люкс С., Жу А., Шамір А..

Алгоритми гешування

- MD-5;
- SHA-1, SHA-2;
- Keccak;
- Luffa, Luffa v2;
- Blue Midnight Wish;
- Skein;
- Blake, Blake 2.

Порівняльна характеристика методів гешування.

Геш-алгоритм	Довжина геш-значення	Максимальна довжина повідомлення	Розмір слова (біти)	Round of Compression	Атаки
Blake-256 Blake-512	256 512	$< 2^{64}$ $< 2^{128}$	32 64	14 16	Знаходження колізій Slide attack
BMW224 BMW224	256 512	$< 2^{64}$ $< 2^{64}$	32 64		Знаходження колізій Знаходження другого прообразу
Skein-256 Skein-512	Підтримує будь-яку довжину	$< 2^{64}$ $< 2^{64}$	64	72 72	Pseudo-Near-Collision
MD5	128	$< 2^{64}$	32	64	Атака «дня нарождення» Знаходження другого прообразу Знаходження прообразу
SHA-1	160	$< 2^{64}$	32	80	Атака «дня нарождення» Знаходження колізій Знаходження другого прообразу Знаходження прообразу
Luffa-256 Luffa-512	256 512	$< 2^{64}$ $<2^{128}$	32 64	31 56	semi-free-start collision free-start preimage distinguisher
Keccak-256 Keccak-512	200 1600	$< 2^{320}$ $< 2^{508}$	64 64	7 8	Атака на перший прообраз

Колізійна атака			
Геш-функція	Вимоги безпеки	Найкраща атака	Дата атаки
MD5	2^{64}	2^{18}	2013-03-25
SHA-1	2^{80}	2^{61}	2005-08-17
SHA256	2^{128}	24 з 64 раундів ($2^{28.5}$)	2008-11-25
SHA512	2^{256}	24 з 80 раундів ($2^{32.5}$)	2008-11-25
Префіксна колізійна атака			
MD5	2^{128}	$2^{123.4}$	2009-04-16
SHA-1	2^{160}	45 з 80 раундів	2008-08-17
SHA256	2^{256}	42 з 64 раундів ($2^{251.7}$)	2008-11-25
SHA512	2^{512}	46 з 80 раундів ($2^{511.5}$)	2008-11-25
Атака на перший прообраз			
MD5	2^{128}	$2^{123.4}$	2009-04-16
SHA-1	2^{160}	45 з 80 раундів	2008-08-17
SHA256	2^{256}	42 з 64 раундів ($2^{251.7}$)	2008-11-25
SHA512	2^{512}	46 з 80 раундів ($2^{511.5}$)	2008-11-25

Загальні атаки

- Дня народження;
- Збільшення довжини повідомлення;
- Келсі-Коно;
- Жу;
- Хоча-Шаміра.

Апаратні засоби представлені на ринку

- RuToken;
- Guardant;
- eToken;
- IRONKEY;
- Altera MAX, Stratix.

Техніко економічне обґрунтування доцільності розробки

Основні технічні показники аналога і нової розробки

Показники	Аналог	Нова розробка	Відношення параметрів нової розробки до параметрів аналога
Кількість тактів на 1 біт даних	4	1,5	Розробка ліпше
Взрасливість до загальних атак	8	2	Розробка ліпше
Криптостійкість	5	7	5/7

Оцінювання комерційного потенціалу розробки

$\overline{СБ}$ = 33

Ітеративне криптографічне перетворення

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

Де q – кількість каналів.

Функція ущільнення для гешування даних

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

де:

- h_i– проміжне геш-значення, отримане на i-му кроці;
- g – примітивний елемент за модулем p;
- m_i– i-й блок даних;

Функція ущільнення для гешування даних

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

де:

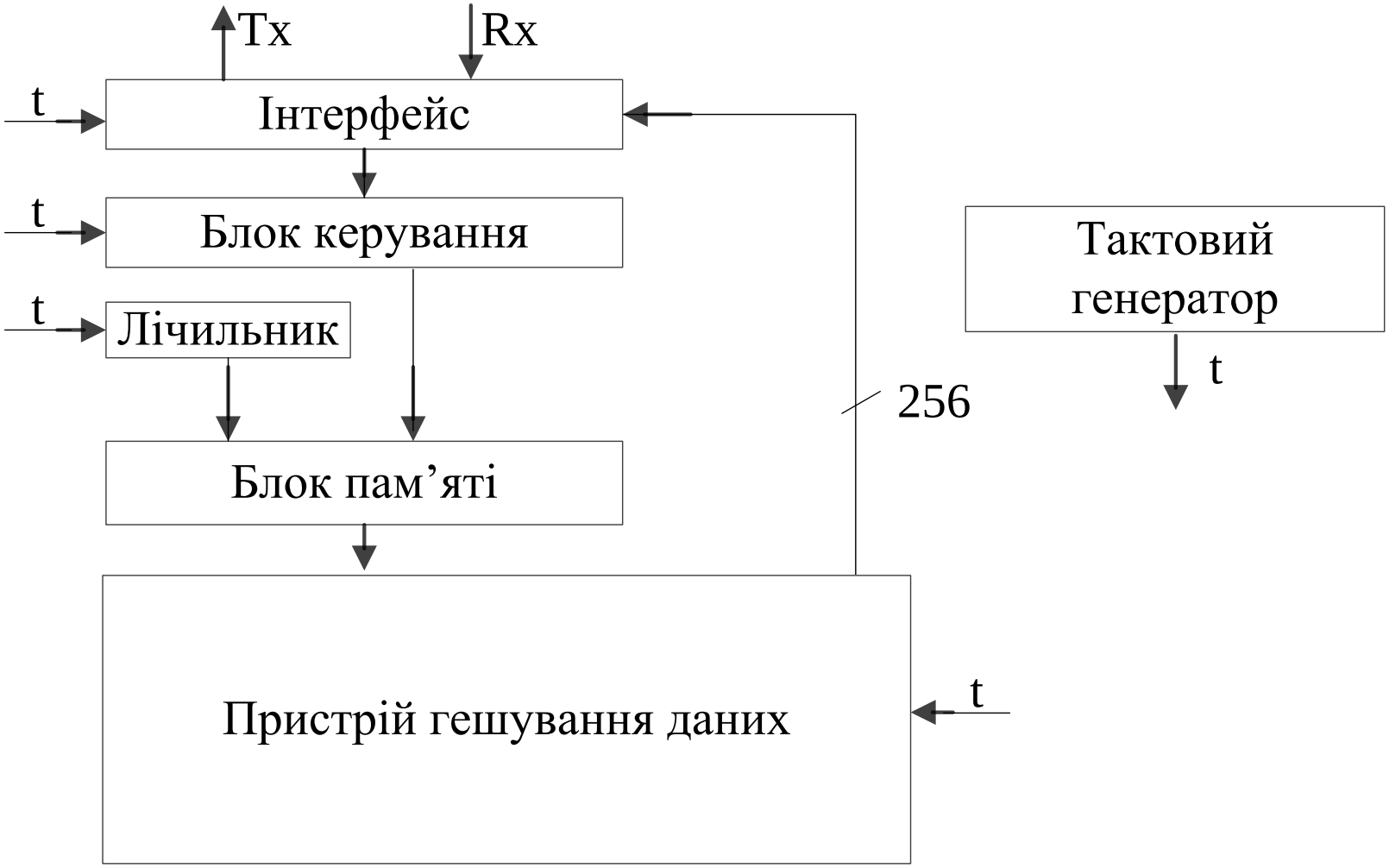
- h_{i-1}^{j} – попереднє проміжне геш-значення, отримане на i-му кроці;

Метод багатоканального гешування

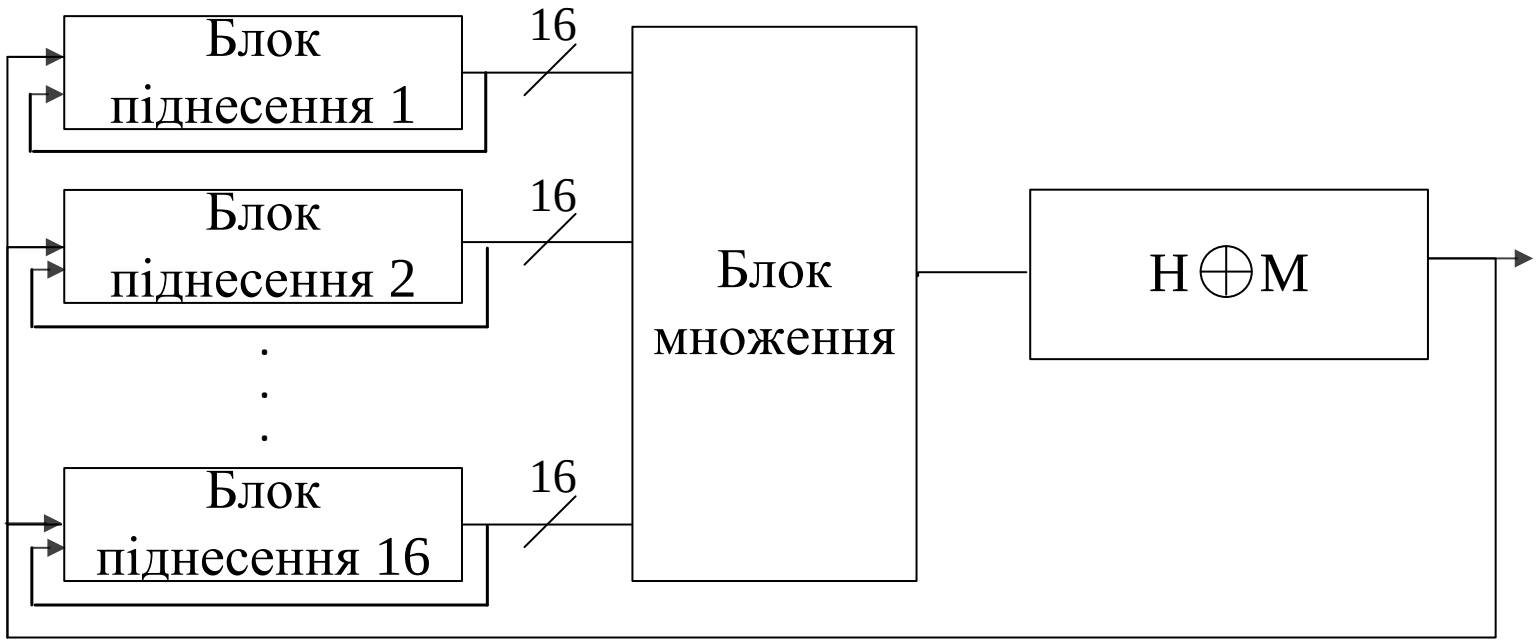
Передбачає такі дії:

- отримання вхідного повідомлення *M* і доповнення його до найменшої довжини, що кратна довжині блоку даних, якщо *M* не кратне *q*-обчислювальним каналам відповідного розряду;
- розбиття вхідного повідомлення *M* на блоки даних рівної довжини ;
- визначення показника степеня на основі повідомлення m_i та геш-значення h_i;
- обчислення проміжного геш-значення, шляхом піднесення примітивного елемента *g* до степеня за модулем *p*;
- множення проміжних геш-значень.
- Повторення кроків 3, 4, 5 поки не закінчиться вхідного повідомлення *M* відповідно до формули 3.4;

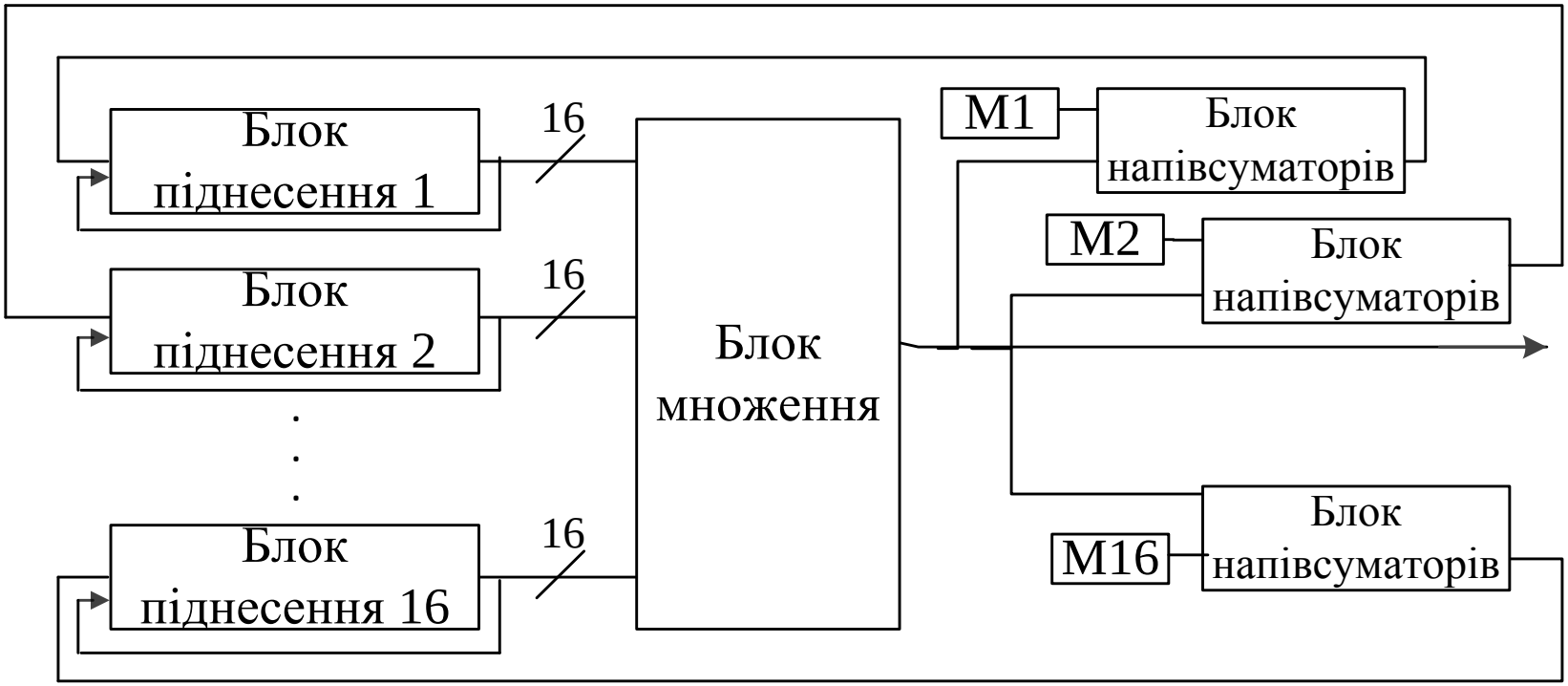
Загальна схема спеціалізованого процесора



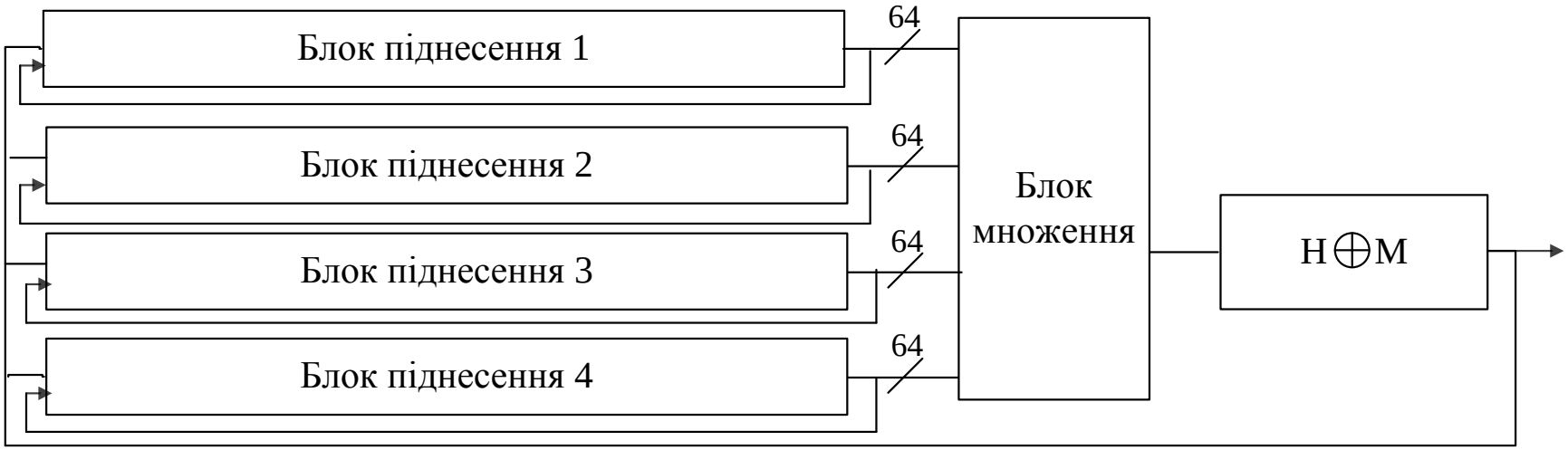
Структура пристрою гешування для методу E16c16



Структура пристрою гешування для методу D16c16



Структура пристрою гешування для методу E256c4



Структура пристрою гешування для методу D256c4

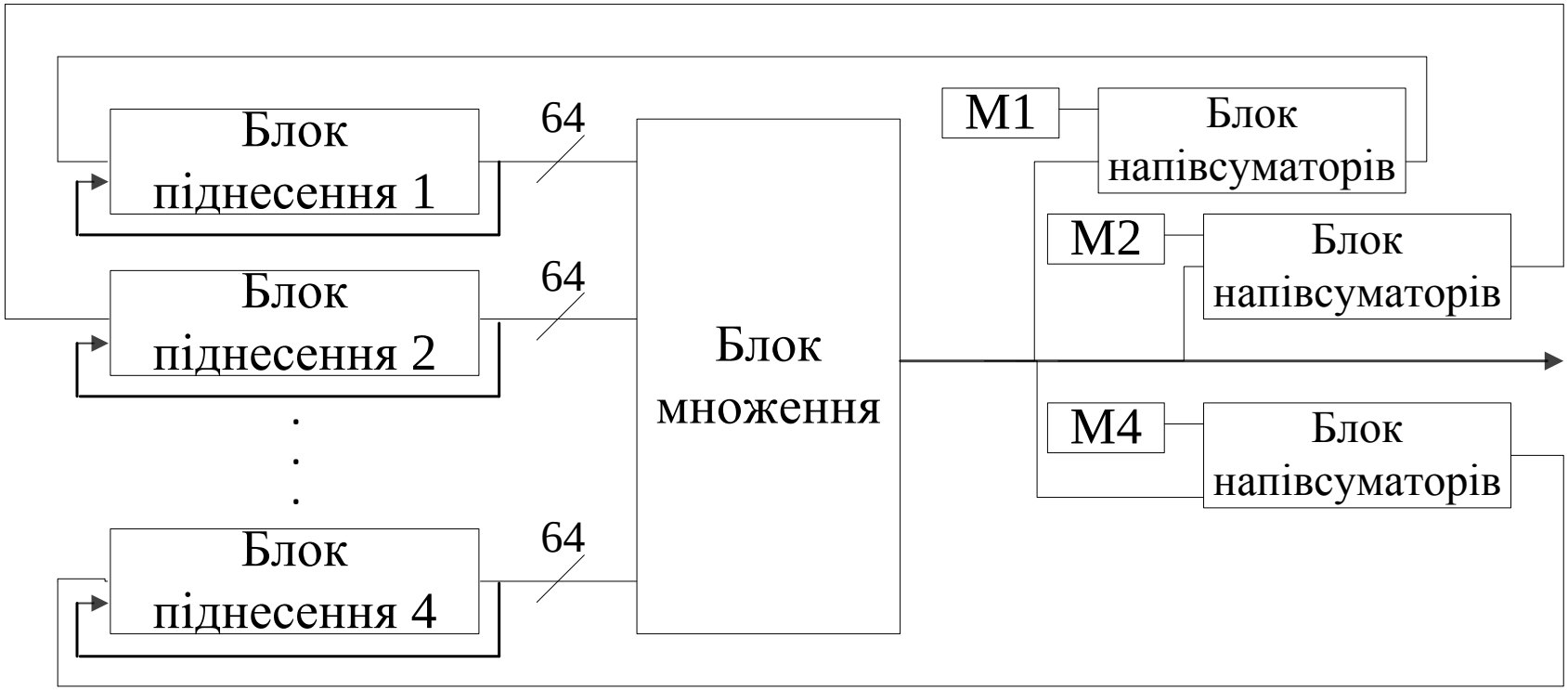
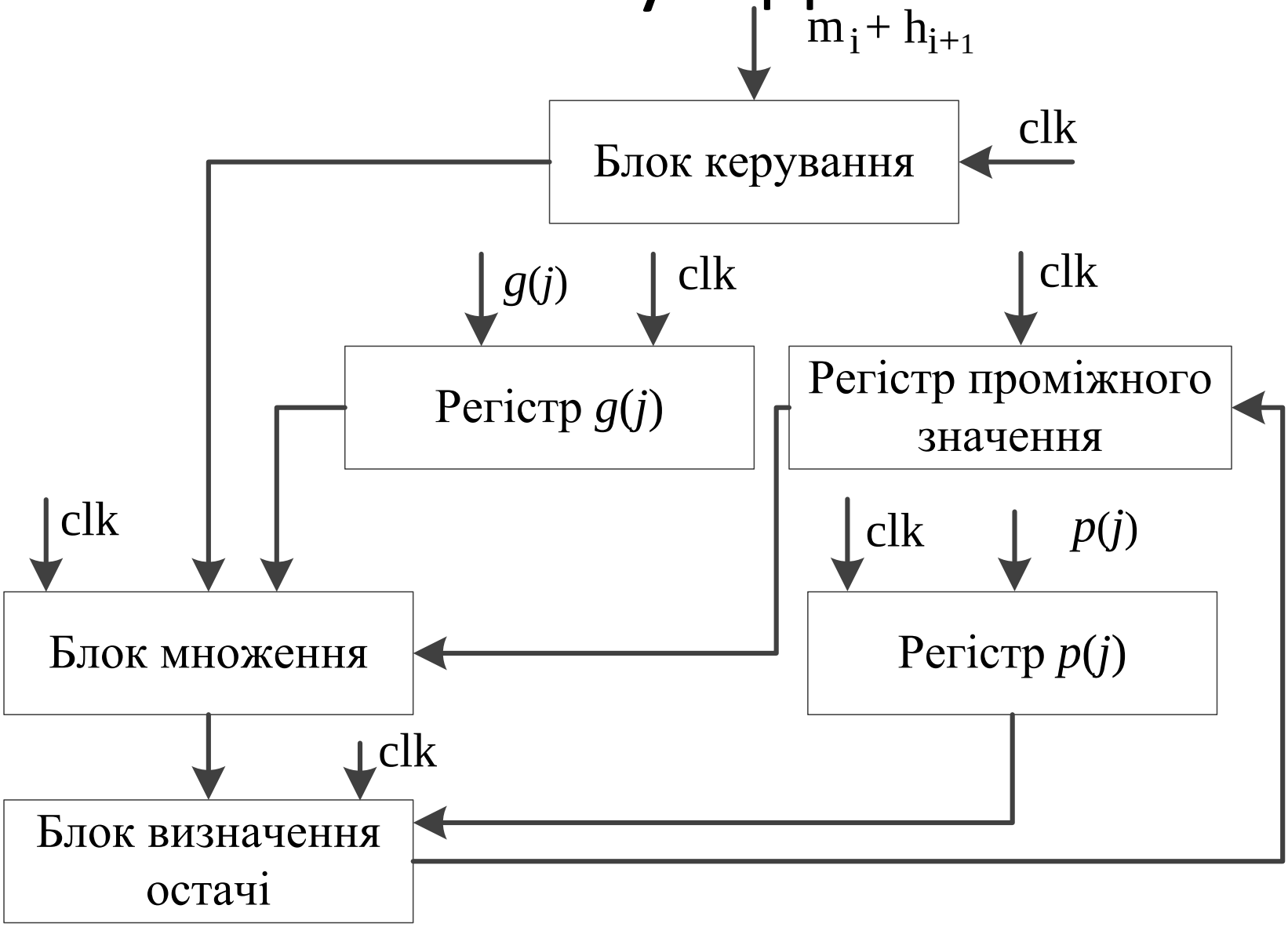
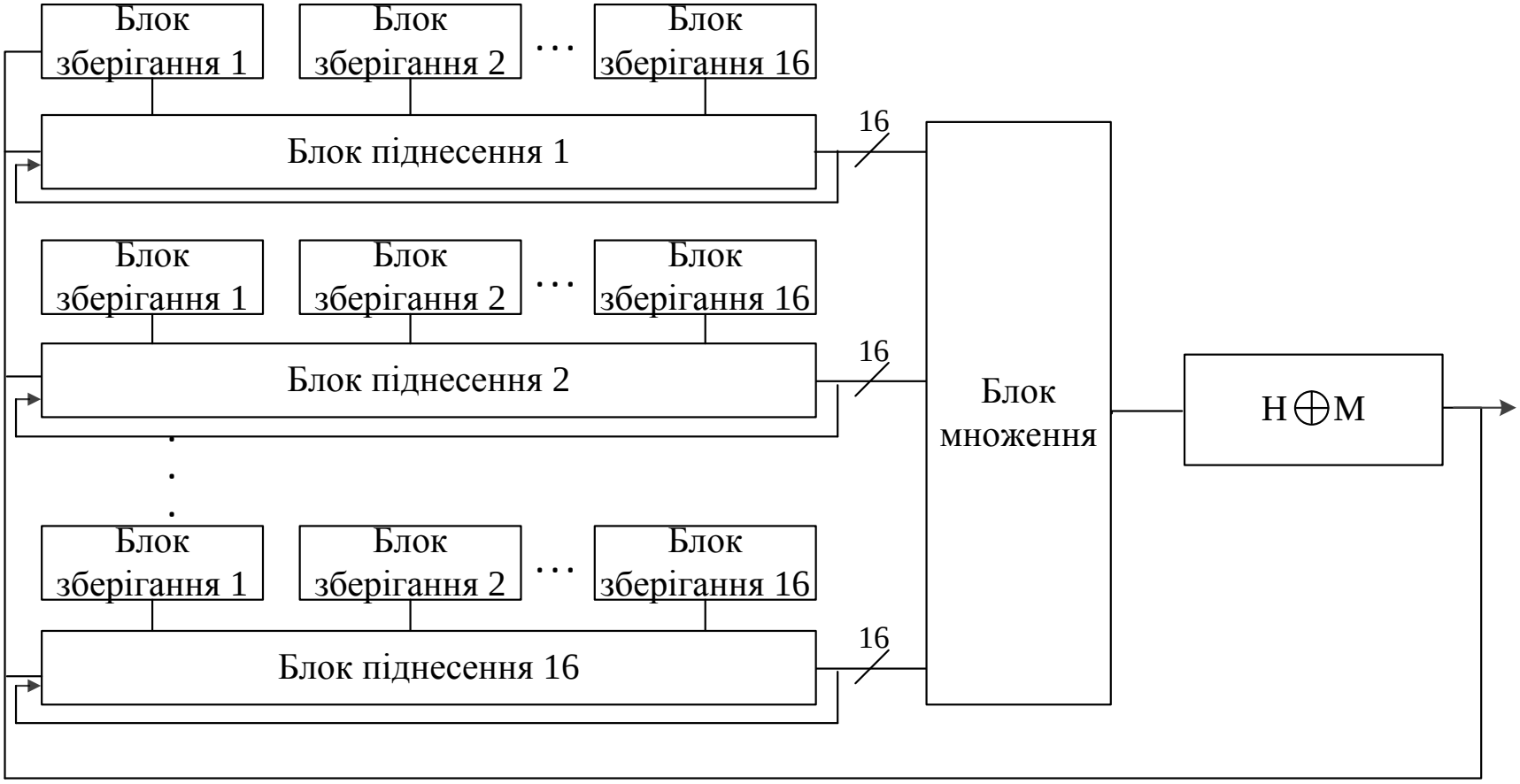


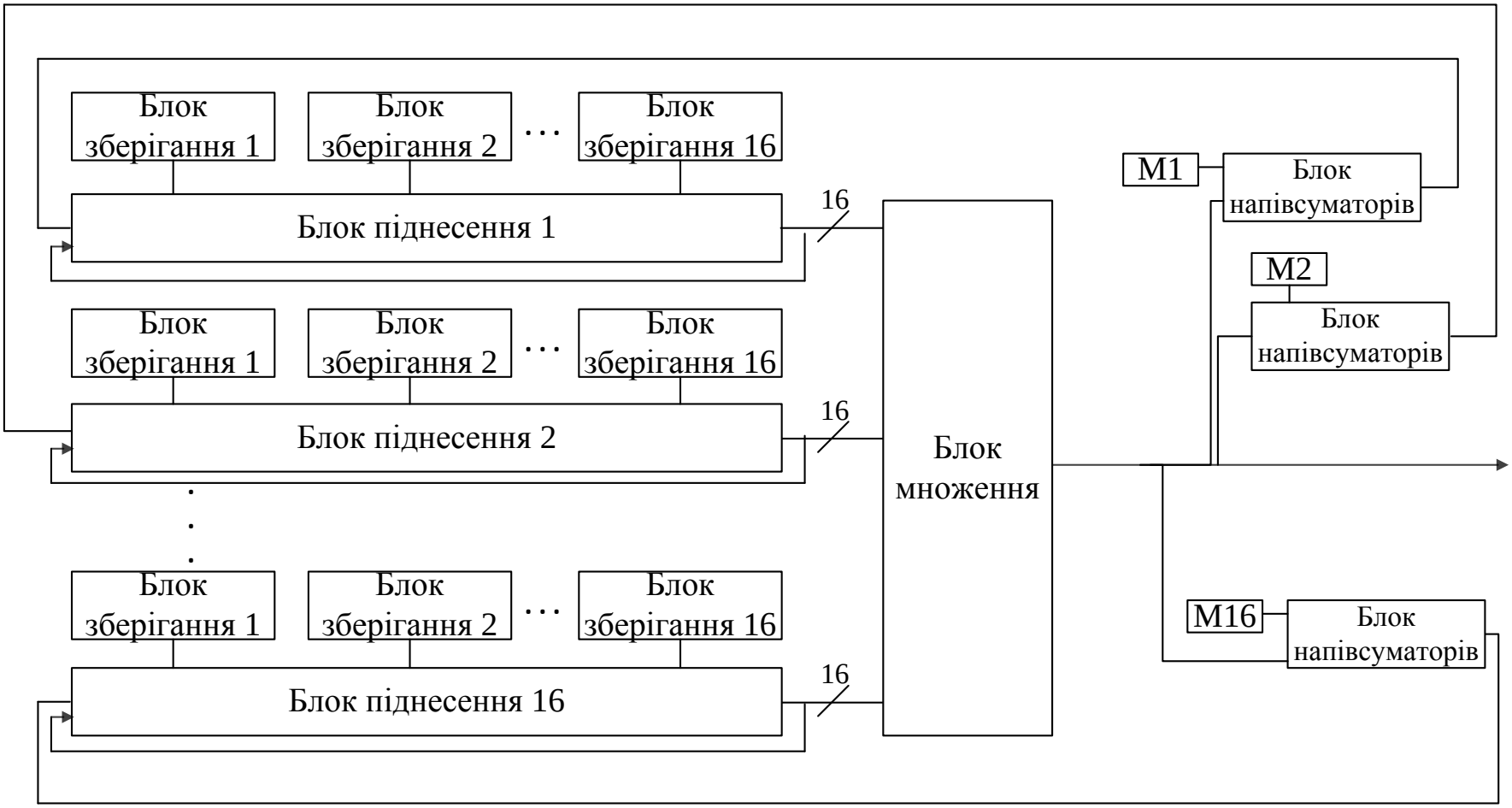
Схема блоку піднесення



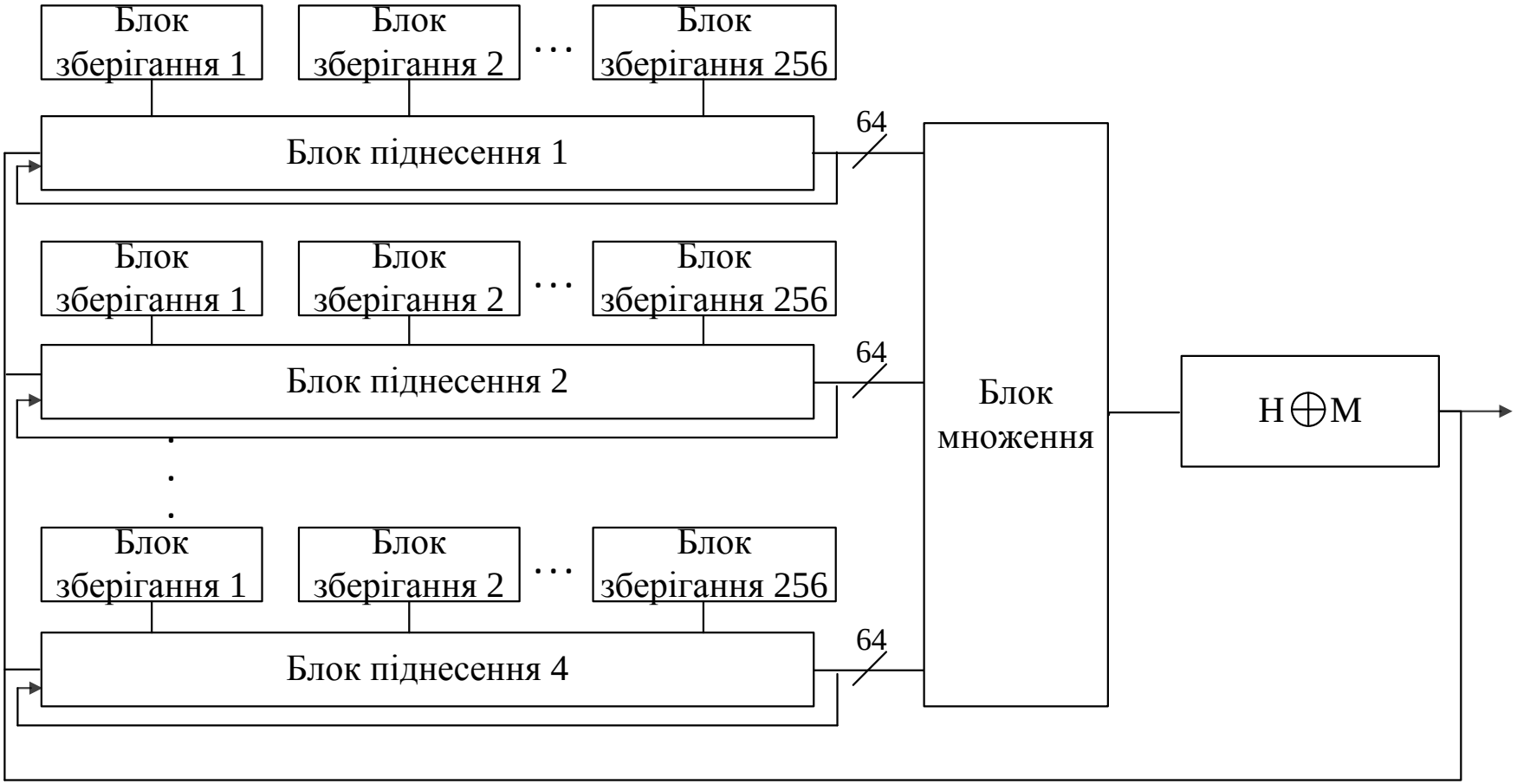
Структура пристрою гешування для методу AE16c16



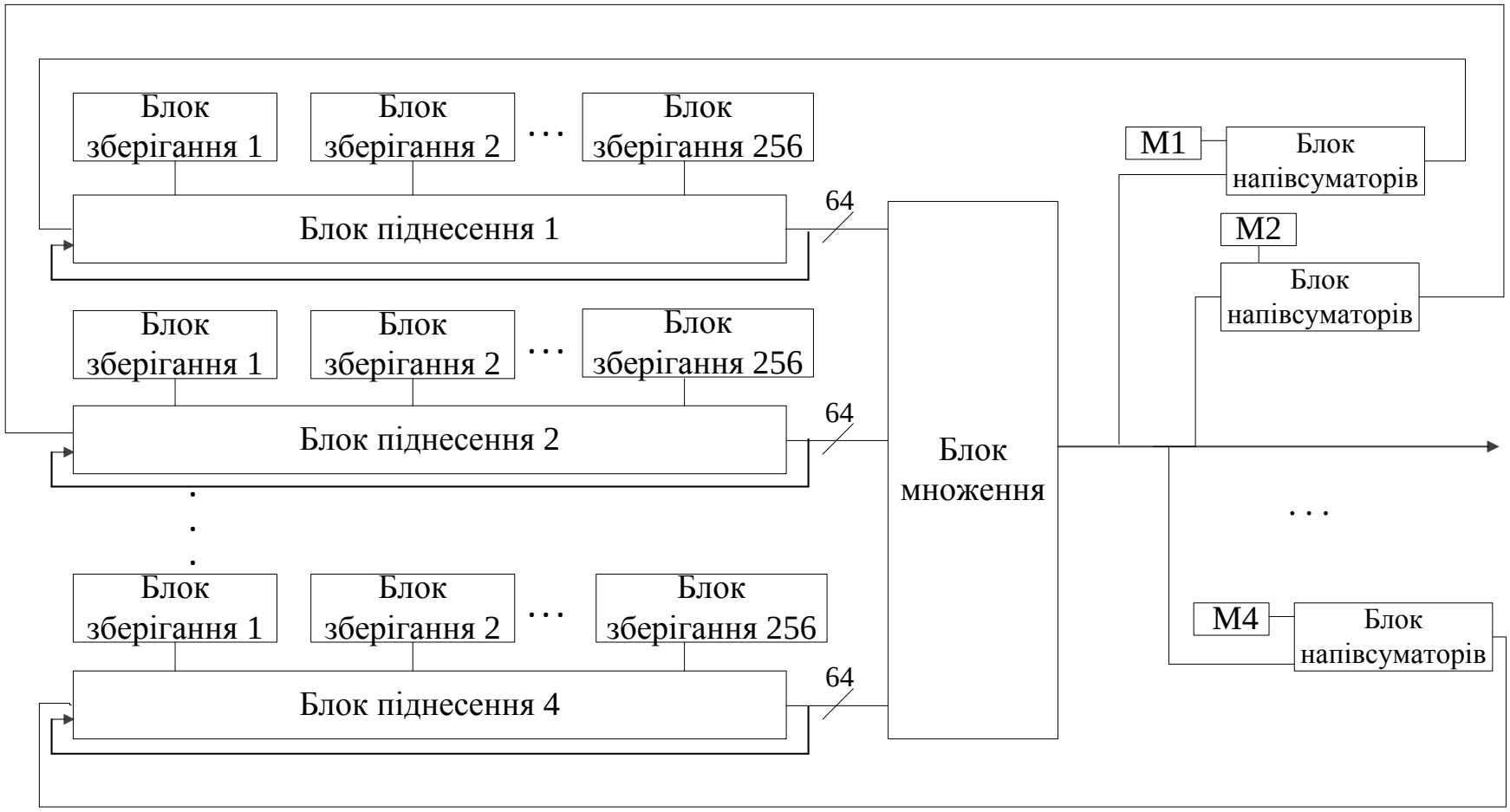
Структура пристрою гешування для методу AD16c16



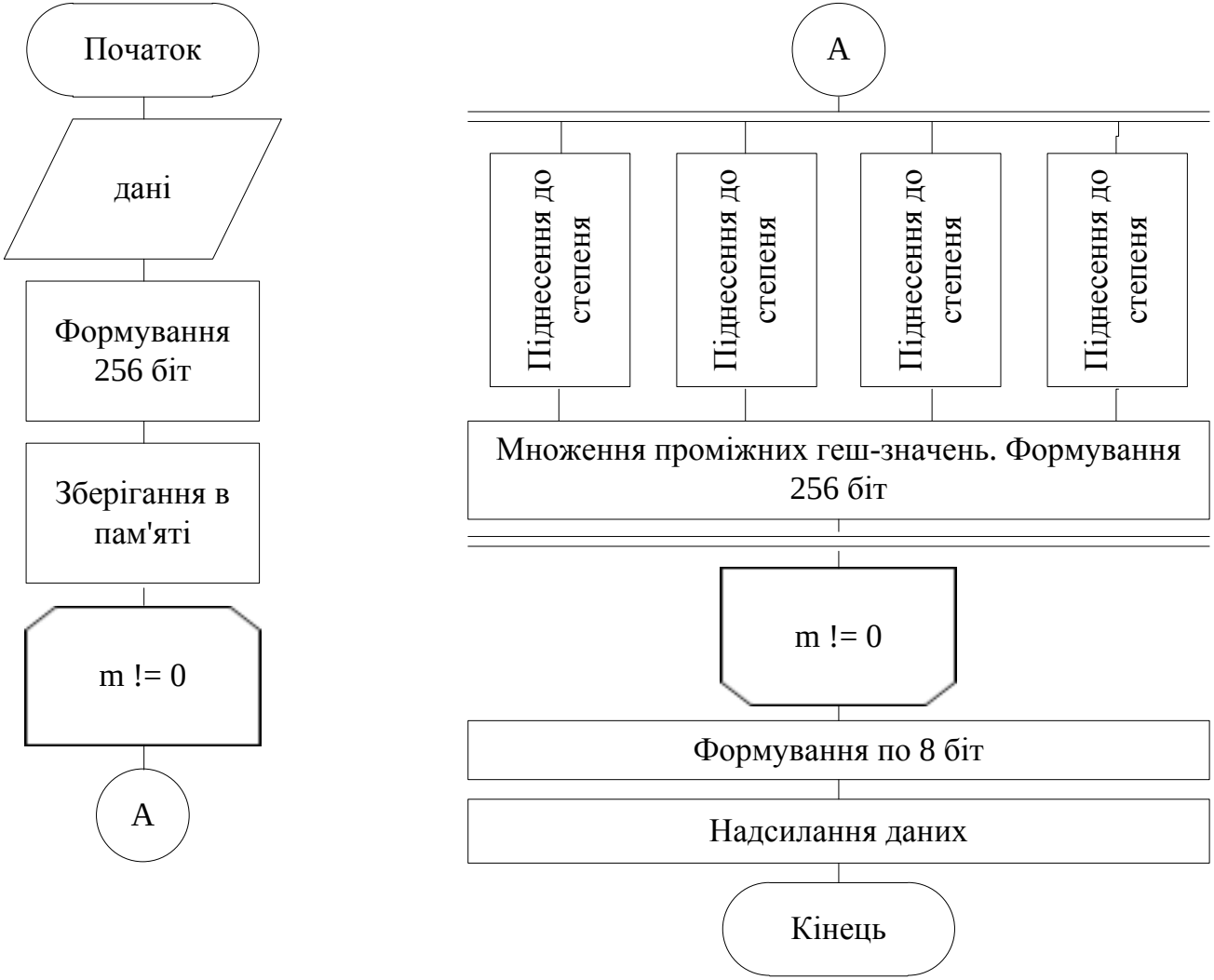
Структура пристрою гешування для методу AE256c4



Структура пристрою гешування для методу AD256c4



Узагальнена схема роботи процесора



Основні сутності процесорів

```
entity ControlBlock is
Port (clk: in bit;
    M : in STD_LOGIC_VECTOR (63 downto 0);
    H : in STD_LOGIC_VECTOR (63 downto 0);
    Stepin : out STD_LOGIC_VECTOR (15 downto
0);
    HiReadyContr : in bit;
    HInit : in bit;
    StartCalcHi: out bit);
end ControlBlock;
```

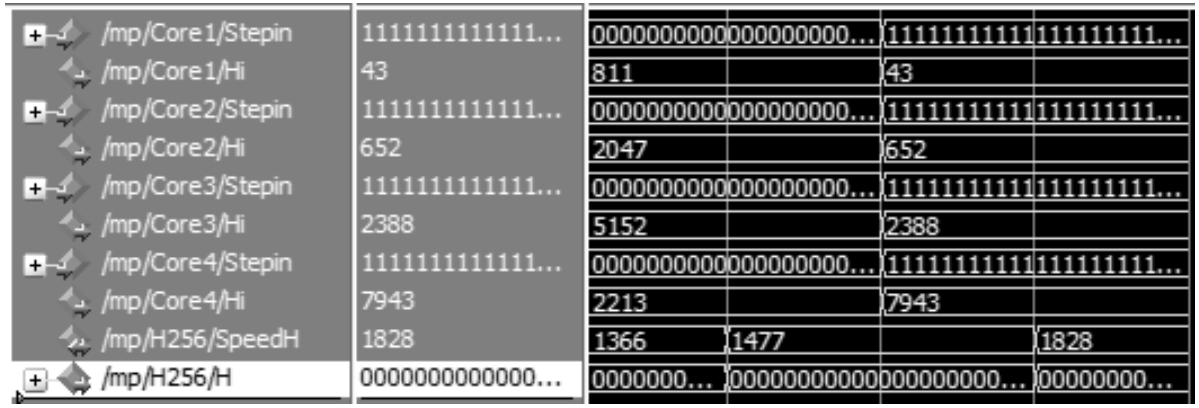
```
entity Calculate_H is
Port (clk: in bit;
    Hi1: in integer;     Hi1Ready: in bit;
     Hi2: in integer;      Hi2Ready: in bit;
      Hi3: in integer;        Hi3Ready: in bit;
       Hi4: in integer;          Hi4Ready: in bit;
            HInit : out bit;
    H : out STD_LOGIC_VECTOR (63 downto 0));
end Calculate_H;
```

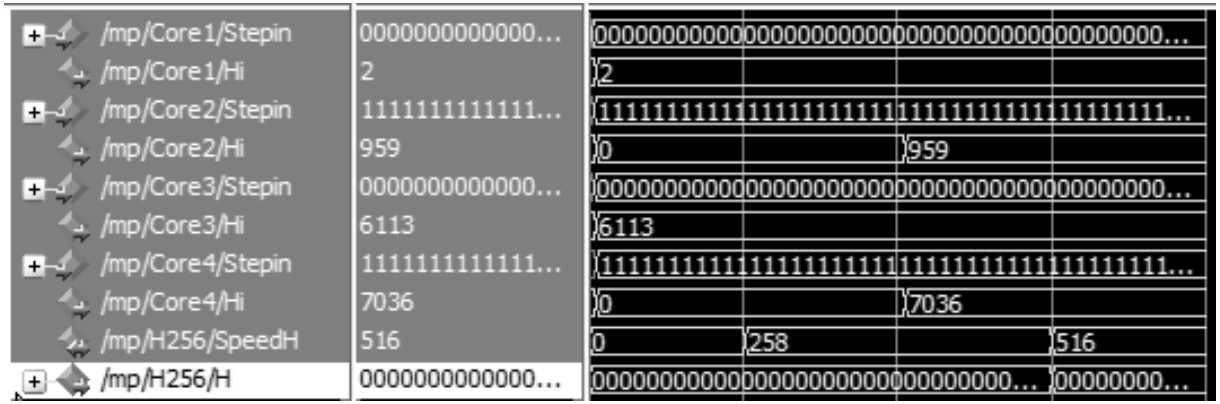
```
entity Calculate_Hi is
Port (--clk: in bit;
      StartCalcHi: in bit;
     Stepin : in STD_LOGIC_VECTOR (15 downto
0);
Hi : out integer;
     HiReady: out bit;
     g : in integer;
     p : in integer);
end Calculate_Hi;
```

```
entity synh is
    port(clk:inout bit);
end synh;
```

```
entity MP is
end MP;
```

Результати експериментальних досліджень процесора





Порівняння швидкодії розроблених методів

Методи	M1024	M2048	M4096	Швидкість циклів/байт
E16C16	3132	6265	12536	24,4
D16C16	2882	5764	11528	22,48
AE16C16	2051	4102	8204	16
AD16C16	1695	3390	6780	13,2
E256C4	1554	3107	6214	12,08
D256C4	456	912	1824	3,56
AE256C4	914	1828	3656	7,12
AD256C4	258	516	1032	2

Економічний ефект

На виконання даної розробки потрібно 21 робочих днів. Дана розробка вважається економічно вигідною, окупність якої становитиме 1,5 роки.

Чистий прибуток буде дорівнювати 293262,75 грн. за три роки.

Наукова новизна полягає в такому:

- удосконалено метод багатоканального гешування підвищеної стійкості до загальних атак, який на відміну від відомих використовує наперед обчислені результати піднесення до степеня кратного степеню 2 за модулем простого числа, що дозволяє підвищити швидкість до 2 разів;
- отримали подальший розвиток методи багатоканального гешування підвищеної стійкості до загальних атак, які на відміну від відомих для генерування наступного проміжного геш-значення в певному каналі використовують проміжне геш-значення повідомлення, отримане на попередній ітерації, та частину проміжного геш-значення, отриману на попередній ітерації в цьому ж каналі, що дозволяє підвищити стійкість до виродження геш-значення в одиницю при використанні операції піднесення до степеня за модулем простого числа як функцію ущільнення.

Практична значимість: структури спеціалізованих процесорів стійких до загальних атак; структури спеціалізованих процесорів стійких до загальних атак підвищеної швидкості; програмний опис структур гешування теоретично доведеної стійкості.

Результати магістерської кваліфікаційної дипломної роботи доповідалися на таких конференціях:

Результати магістерської роботи доповідалися на 3 трьох конференцій. Подано заявку на корисну модель №u 2015 02325.

Дякую
за увагу