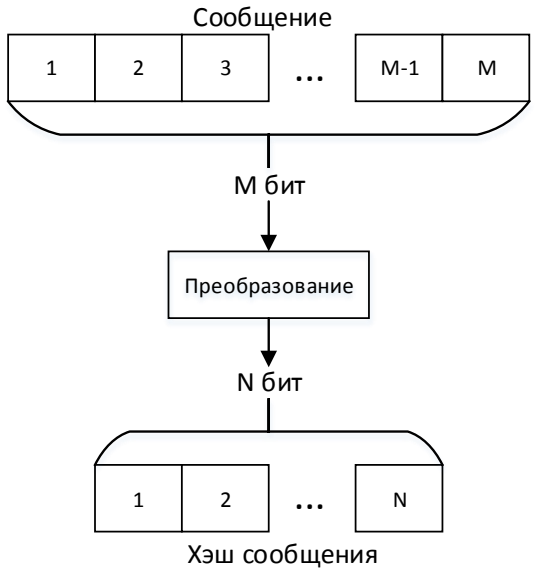
Конвейерный процессор алгоритма хэширования MD5 на базе FPGA

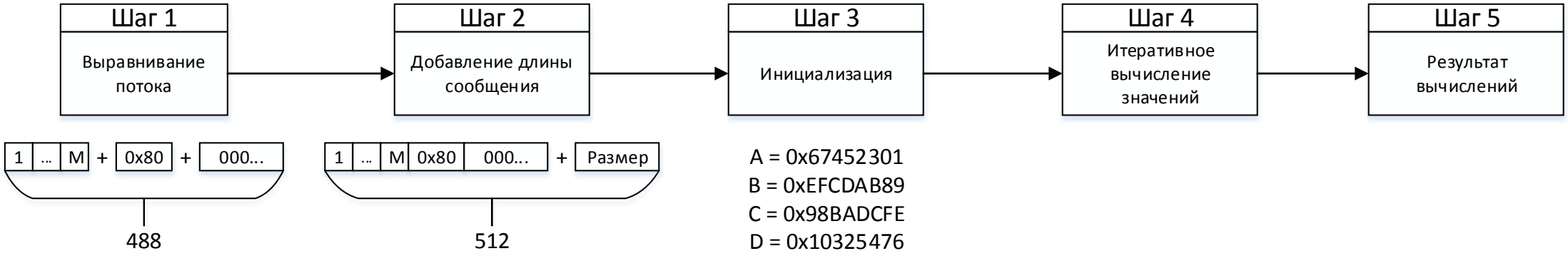
В.Ю. Герасимович, М.В. Качинский, А.В. Станкевич

MD5 – общие сведения

- Автор – Рональд Р. Ривест, 1991 год;
- Алгоритм предназначен для создания отпечатков (хеш-функция) сообщения;
- Хеш – отображение сообщения произвольной длинны на n-разрядную последовательность.



Алгоритм MD5: общая концепция

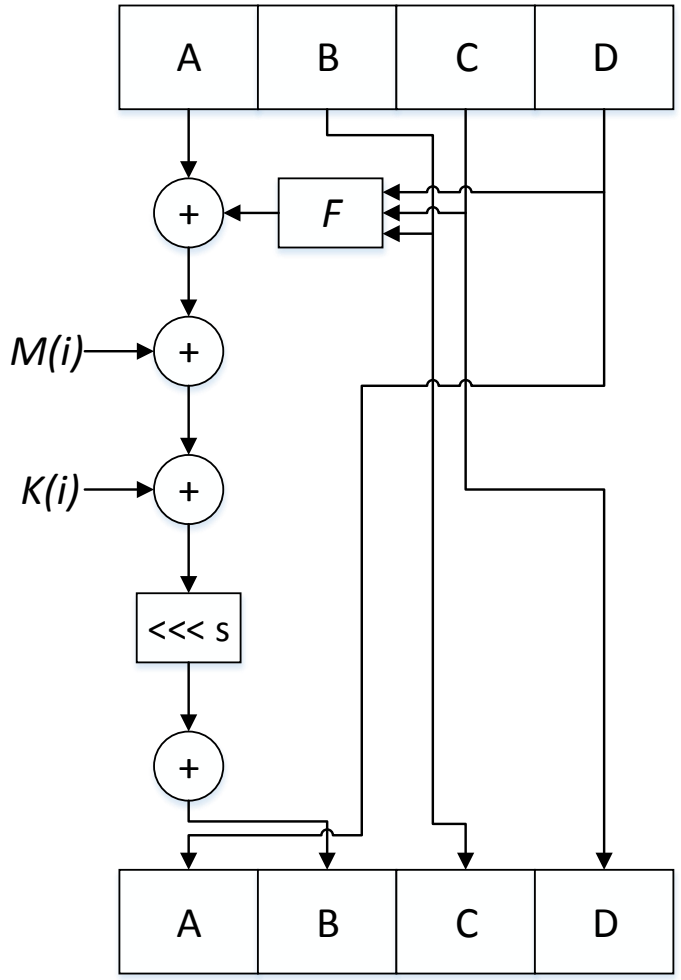


A = 0x67452301
B = 0xEFCDAB89
C = 0x98BADCFE
D = 0x10325476

$$F_1 = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$F_2 = (X \wedge Z) \vee (\neg Z \wedge Y)$$
$$F_3 = X \oplus Y \oplus Z$$
$$F_4 = Y \oplus (\neg Z \vee X)$$

$$K(i) = \text{int}(2^{32} \cdot |\sin(i)|), i = 1...64$$

Алгоритм MD5: шаг вычисления значений



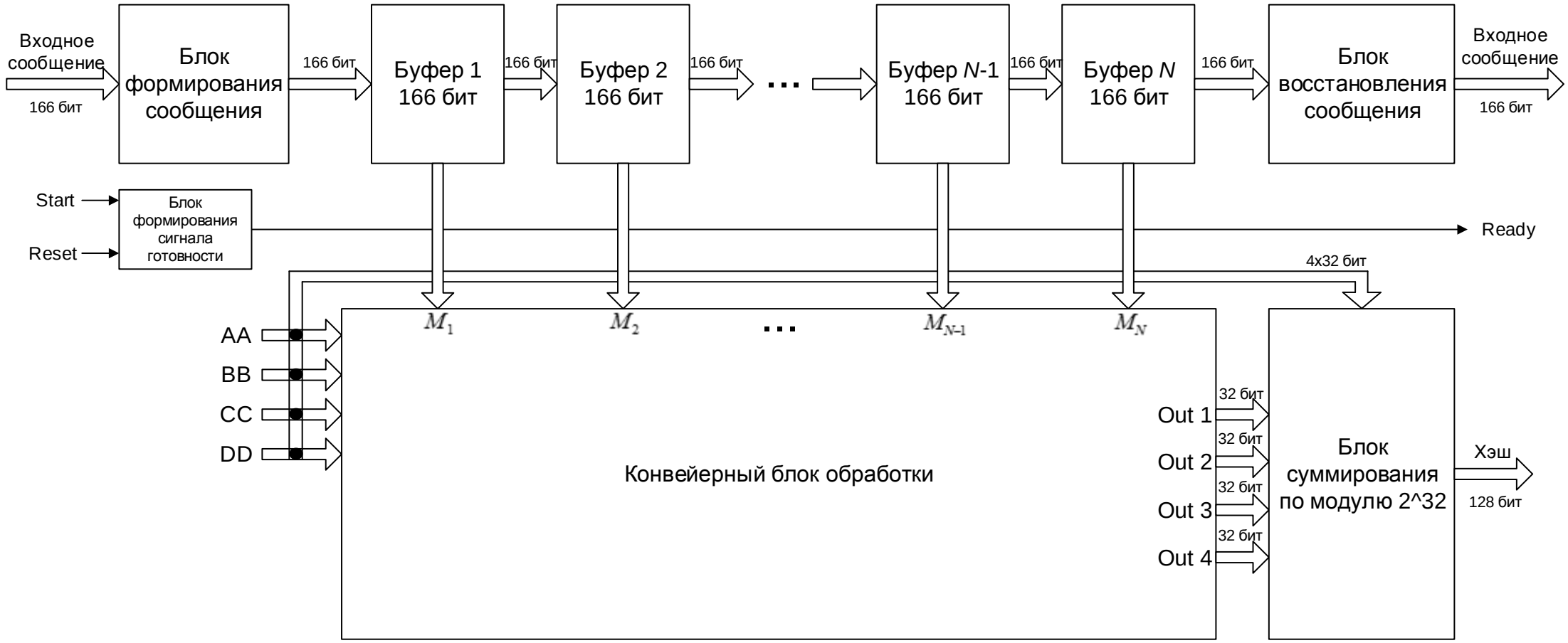
- 4 раунда по 16 шагов вычисления значений;
- индивидуальная функция *F* для каждого раунда;
- различный порядок выборки слов сообщения для раунда (слово – 32 разряда входного сообщения);
- индивидуальный набор значений сдвига *s* для каждого раунда (по 4 значения для раунда).

Конвейерная реализация алгоритма MD5

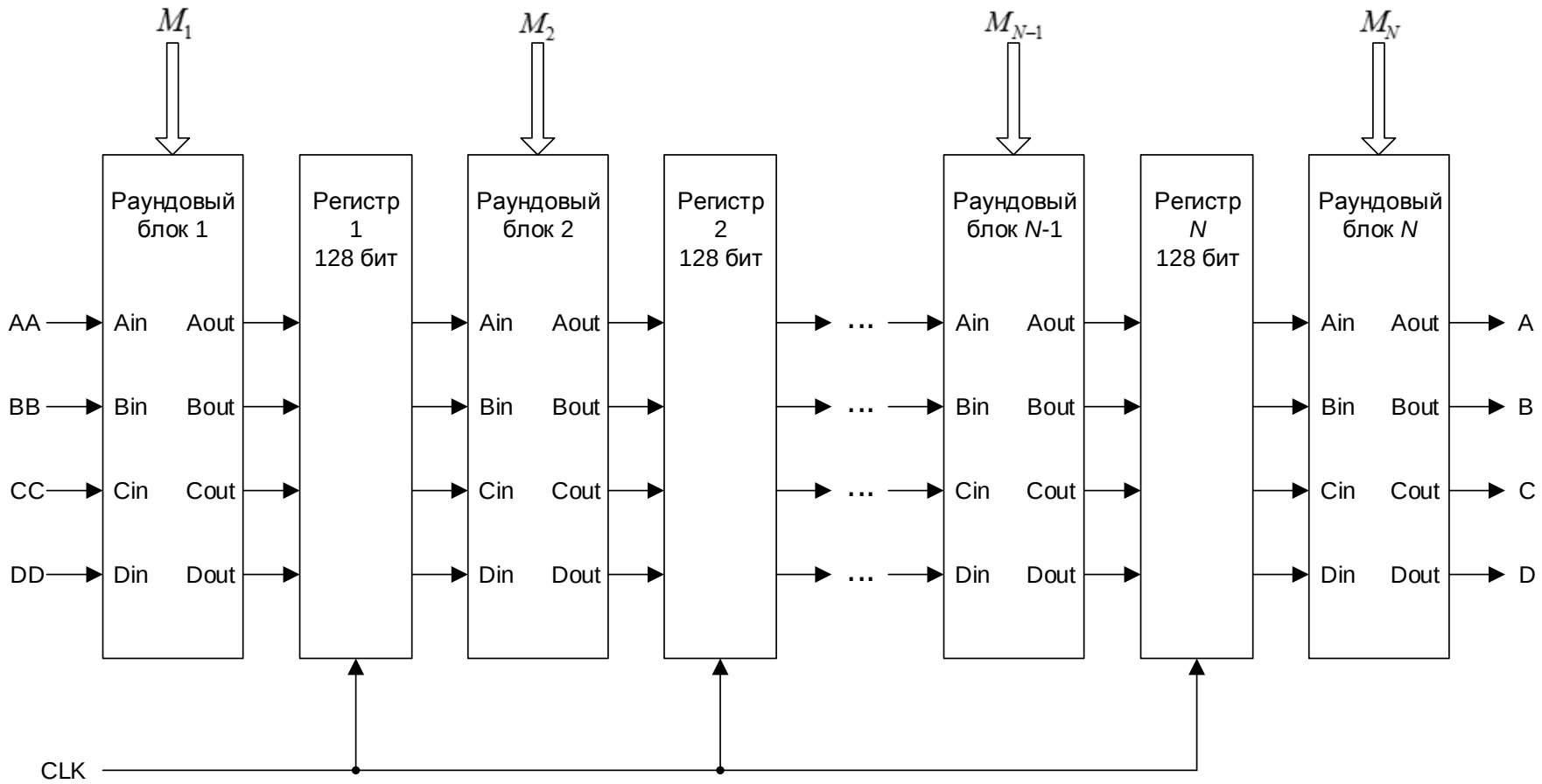
3 типа конвейерной реализации:

- ✓ 4-х ступенчатый конвейер – ступенью конвейера является один раунд алгоритма;
- ✓65-ти ступенчатый конвейер – ступенью конвейера является один шаг работы алгоритма;
- ✓129-ти ступенчатый конвейер – шаг работы алгоритма разбивается на две части, которые вычисляются на соседних ступенях конвейера.

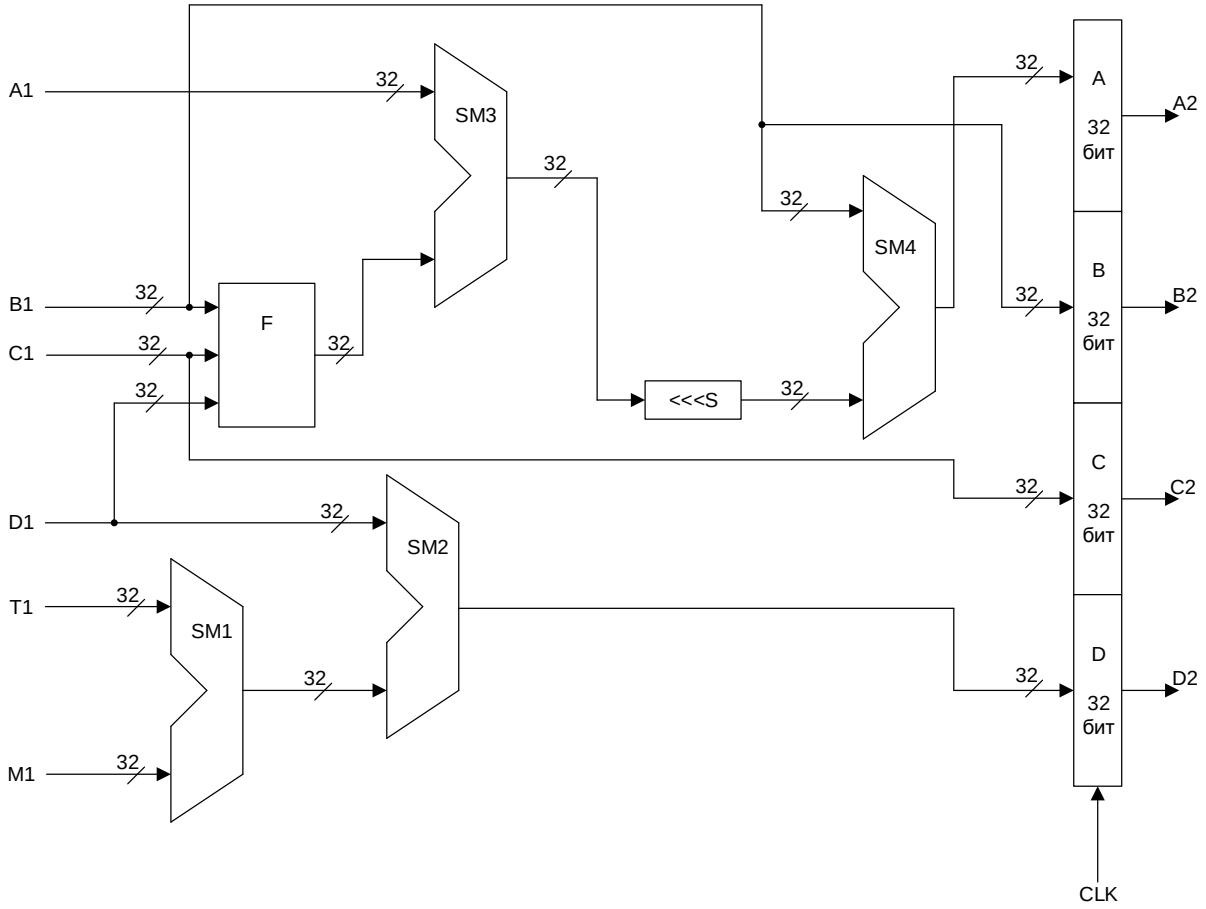
Конвейерная архитектура процессора



Конвейерный блок процессора

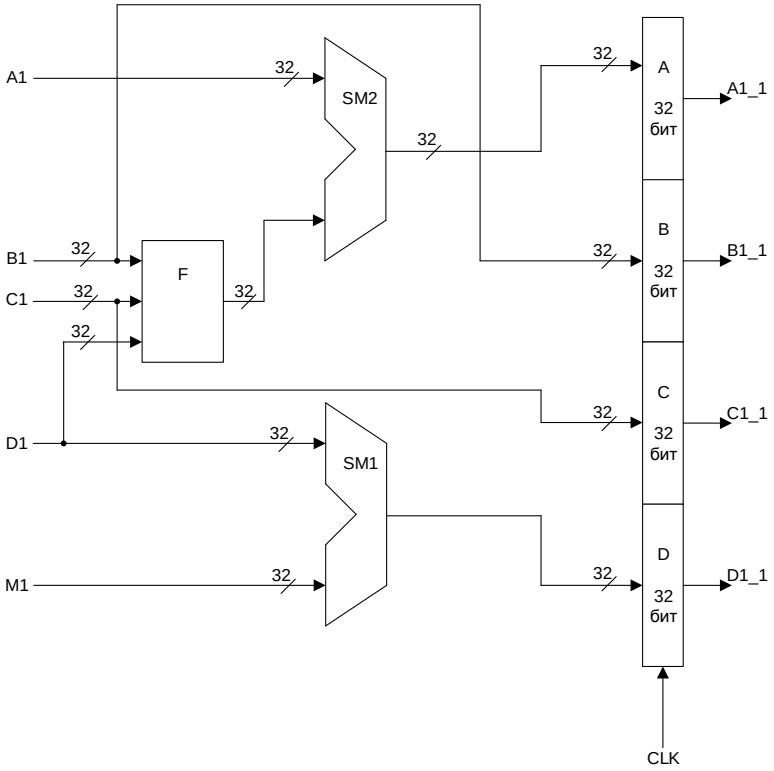


Ступень конвейера: 65-ти ступенчатый конвейер

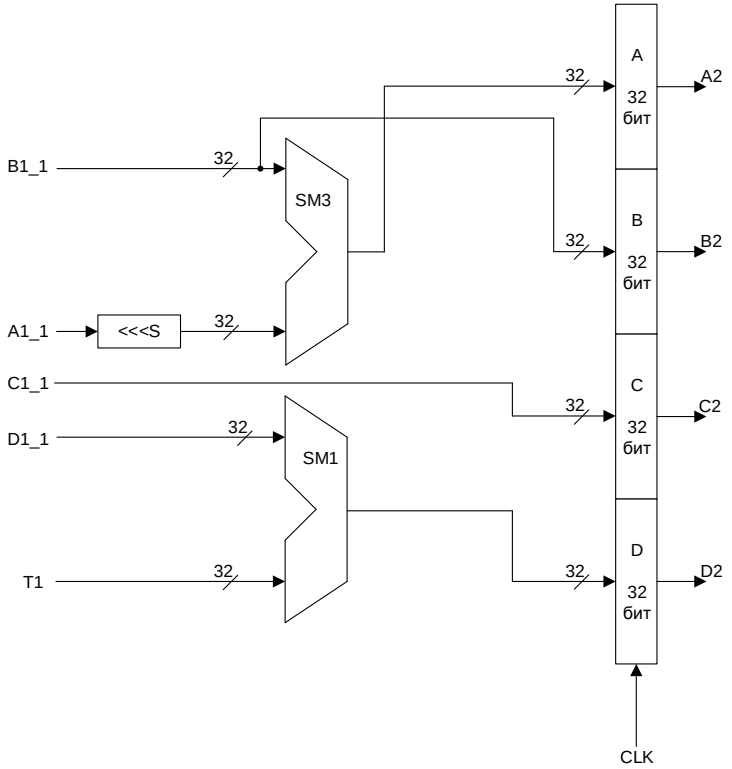


Ступень конвейера: 129-ти ступенчатый конвейер

Ступень конвейера



Промежуточная ступень конвейера



Аппаратные затраты и производительность

Характеристика	Варианты конвейерного процессора		
	На уровне раундов	65 ступеней	129 ступеней
Триггеры	2341 (3%)	9090 (13%)	14967 (21%)
Просмотровые таблицы (LUT)	2069 (2%)	7033 (10%)	10445 (15%)
Секции (slice)	801 (4%)	2812 (16%)	4055 (23%)
Тактовая частота, МГц	167	199	325
Пропускная способность, Гбит/с	4,5	101,9	166,4

Спасибо за внимание!