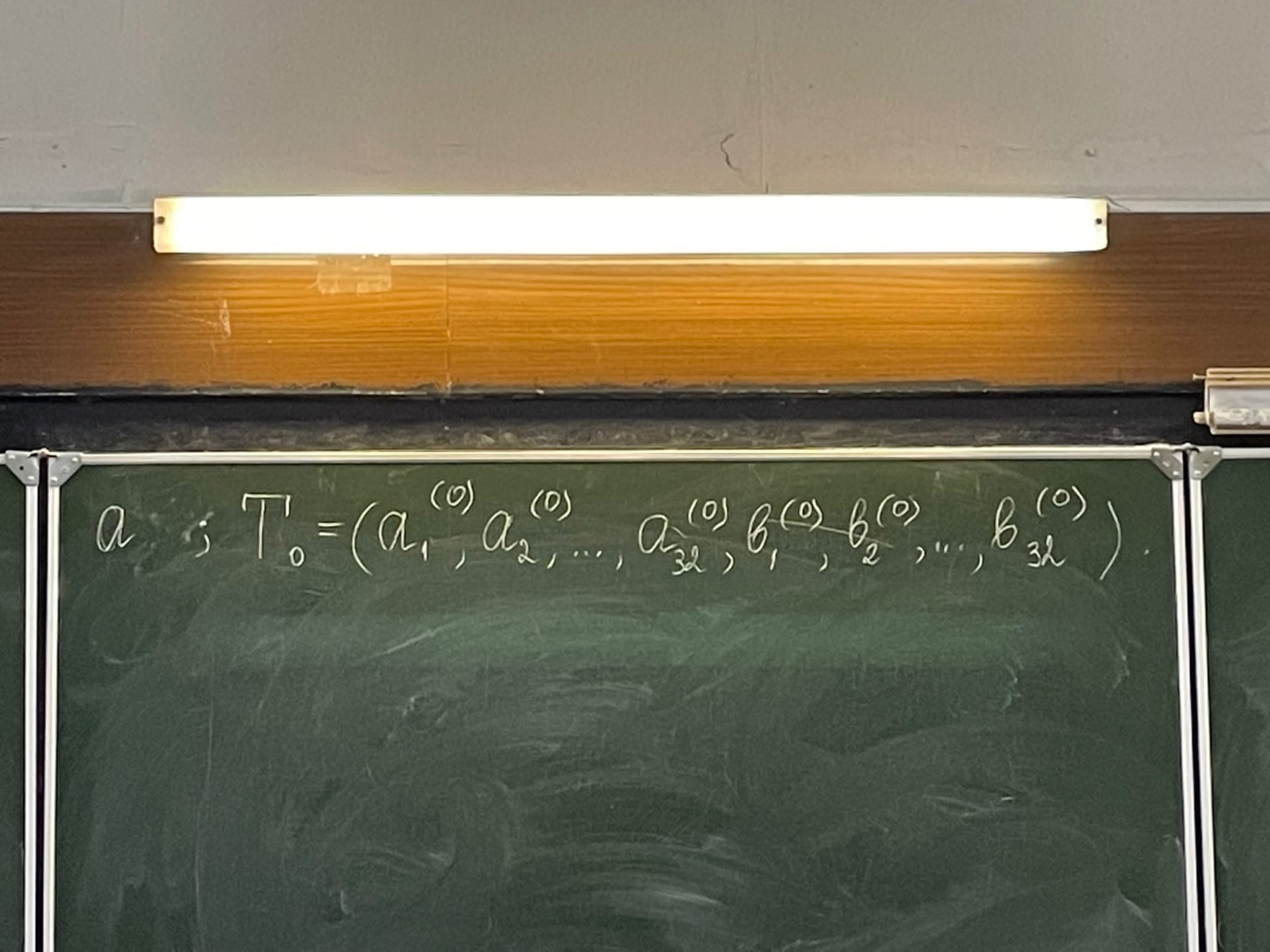
Последовательность битов блока а1(0); To = (a1(0), a2(0), …, a32(0)

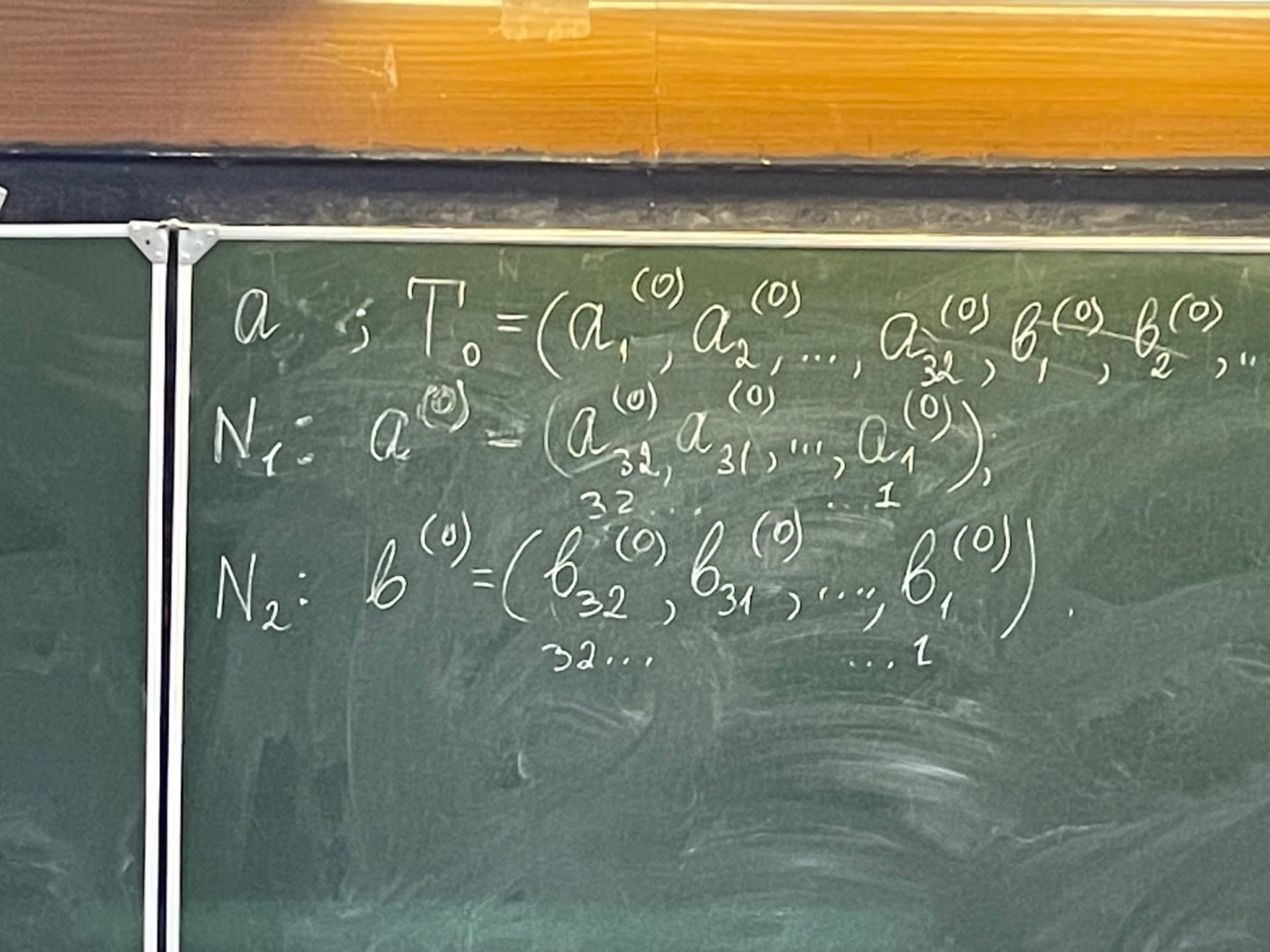


Последовательность блоков битов разби

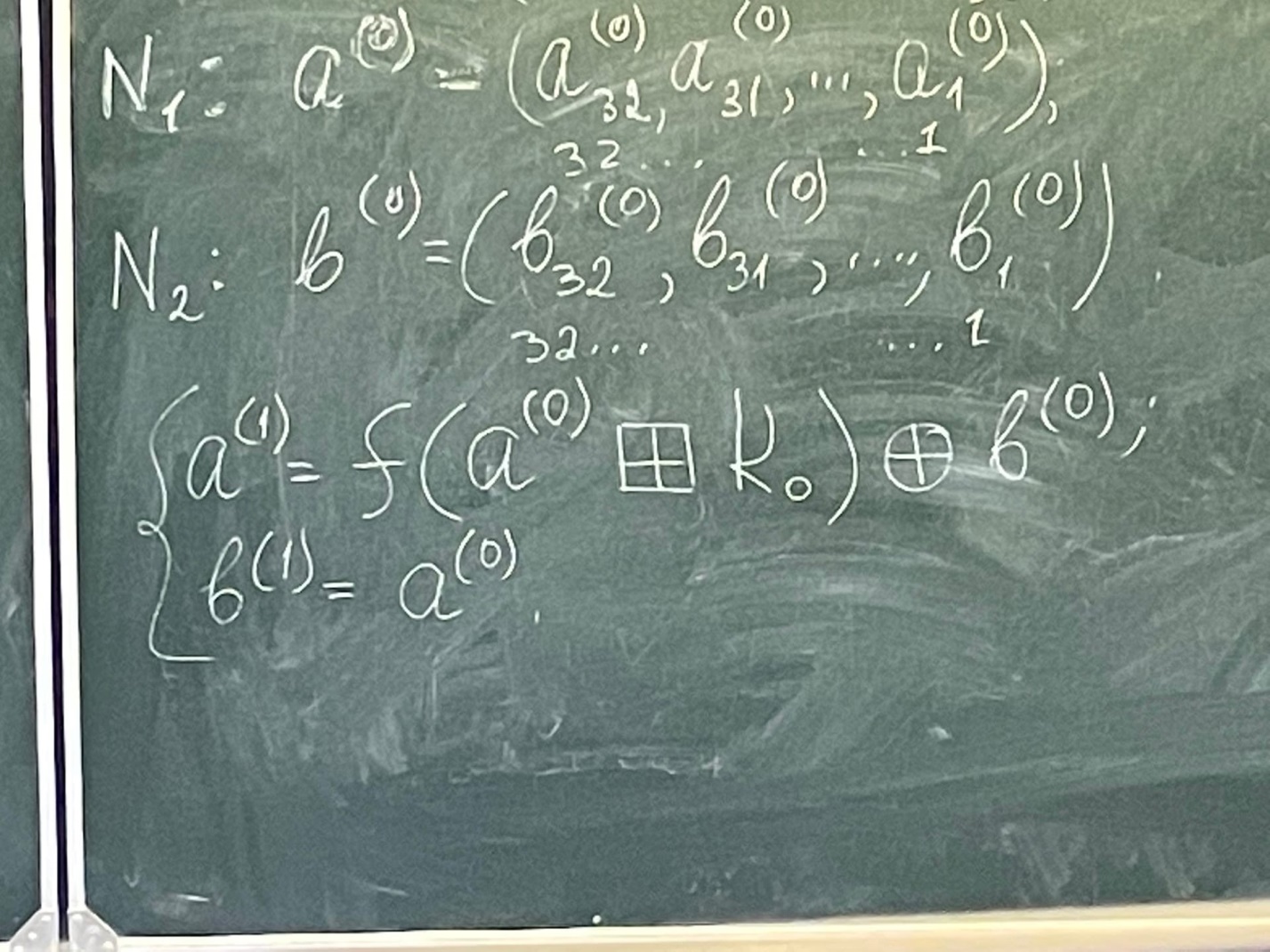
Где b0 левые и старшие биты и ао правые и младшие биты. Эти последовательности вводят в накопители n1 и n2 перед началом первого цикла шифрования.

В результате начальное заполнение n1 будет следующее:

В результате начальное заполнение n2 будет следующее:



Первый цикл (g=1) процедуры шифр-я 64-х разрядного блока можно описать след уравнениями:



В формулах а1 заполнение накопителя n1 после 1 цикла шифрования, b1 заполнение n2 после первого цикла шифрования. F – функция шифрования

Аргументом f является сумма mod 2^32 число a0 (начальное заполнение накопителя n1) и числа Ко - подключа, считываемого из накопителя КЗО.

Каждое из этих чисел = 32 бита.

F включает 2 операции над полученной 32-х разрядной суммой.

1) операция подстановка(замена) выполняется блоком подстановки S

Блок подстановки s состоящий из 8 узлов замены(s блоков замены) с памятью 64 бита каждый. Поступающий из sm1 на блок подстановки s 32-разрядный вектор разбивается на 8 последовательно идущих 4-х разрядных вектора, каждый из которых преобразуется в другой 4-х разрядный вектор соответствующим узлом замены, каждый узел замены можно представить в виде таблицы-перестановки 16 четырёхразрядных двоичных чисел в диапазоне от 0000 до 1111. Входной вектор указывает адрес строки в таблице, а число в этой строке является выходным вектором. Все 8 s блоков различны и являются доп ключевой материал. Затем 4-х разрядные выходные векторы последовательно объединяются в 32-х разрядный вектор. Узлы замены(таблицы-перестановки) представляют собой ключевые элементы которые являются общими для сети эвм и редко перетавляются\*. Эти узлы замены должны сохраняться в секрете.

Функционирование s-блока подстановки

Входной 32х разрядный вектор V содержит 8 4хразрядных векторов Vi

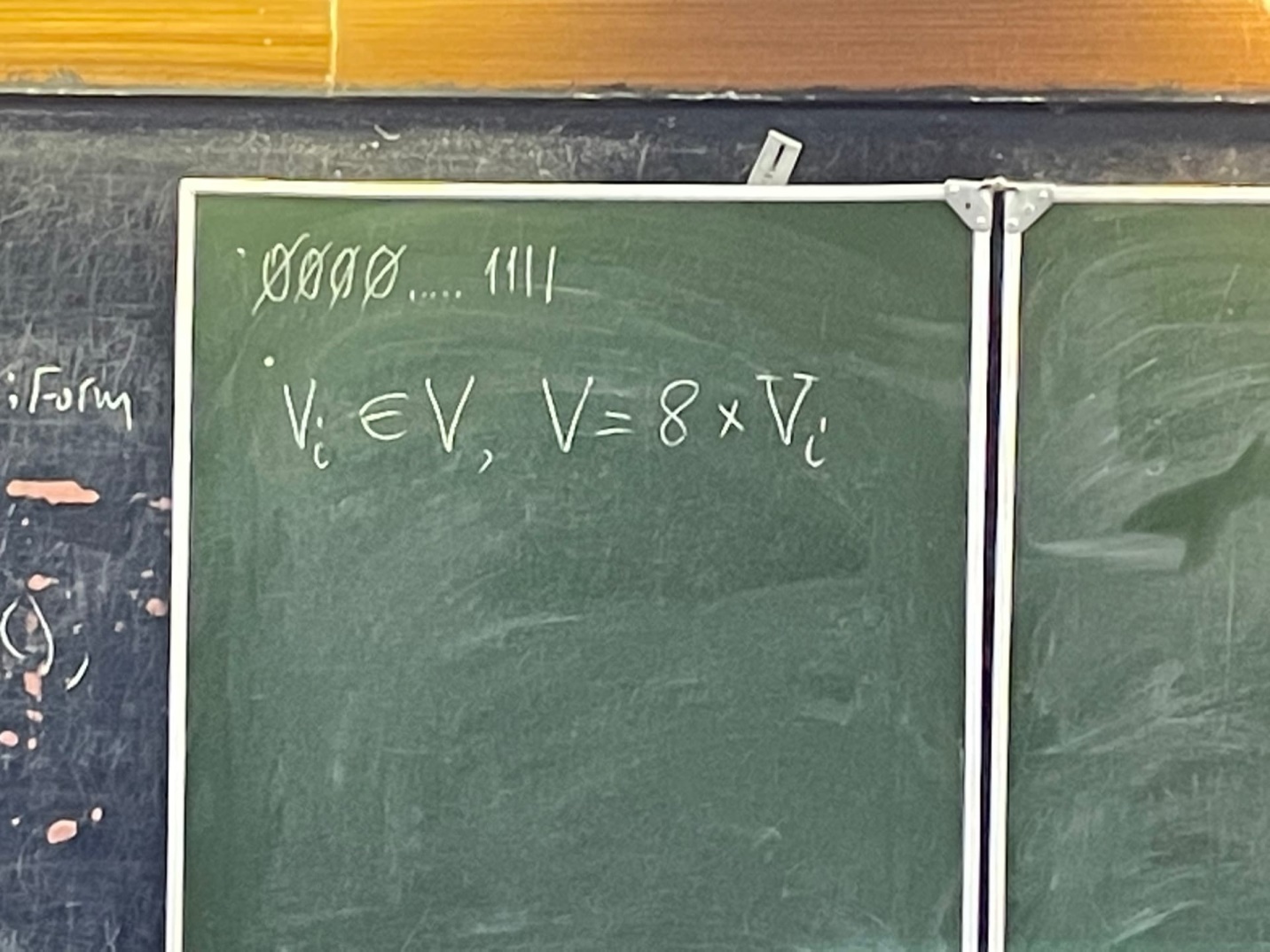
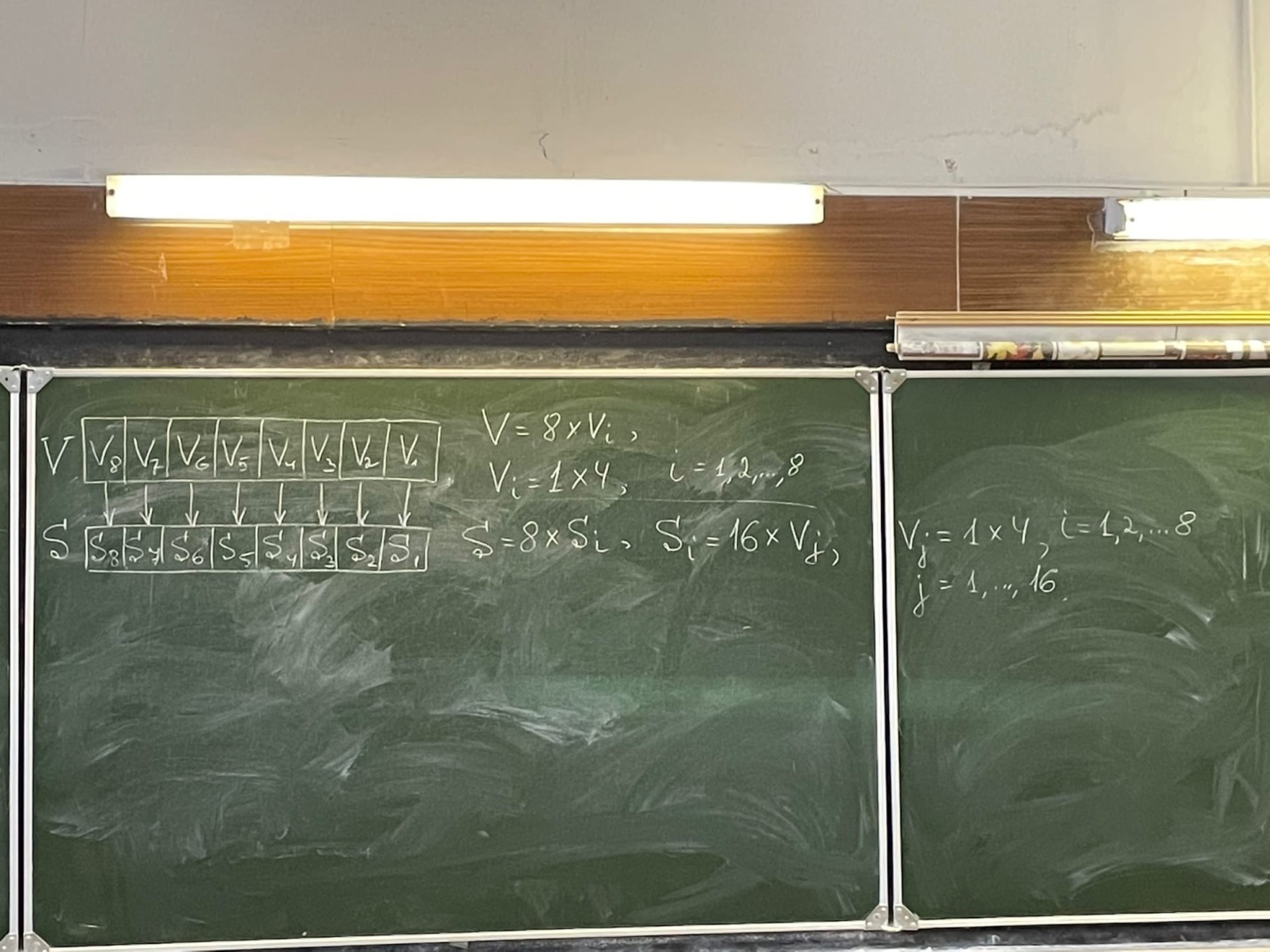


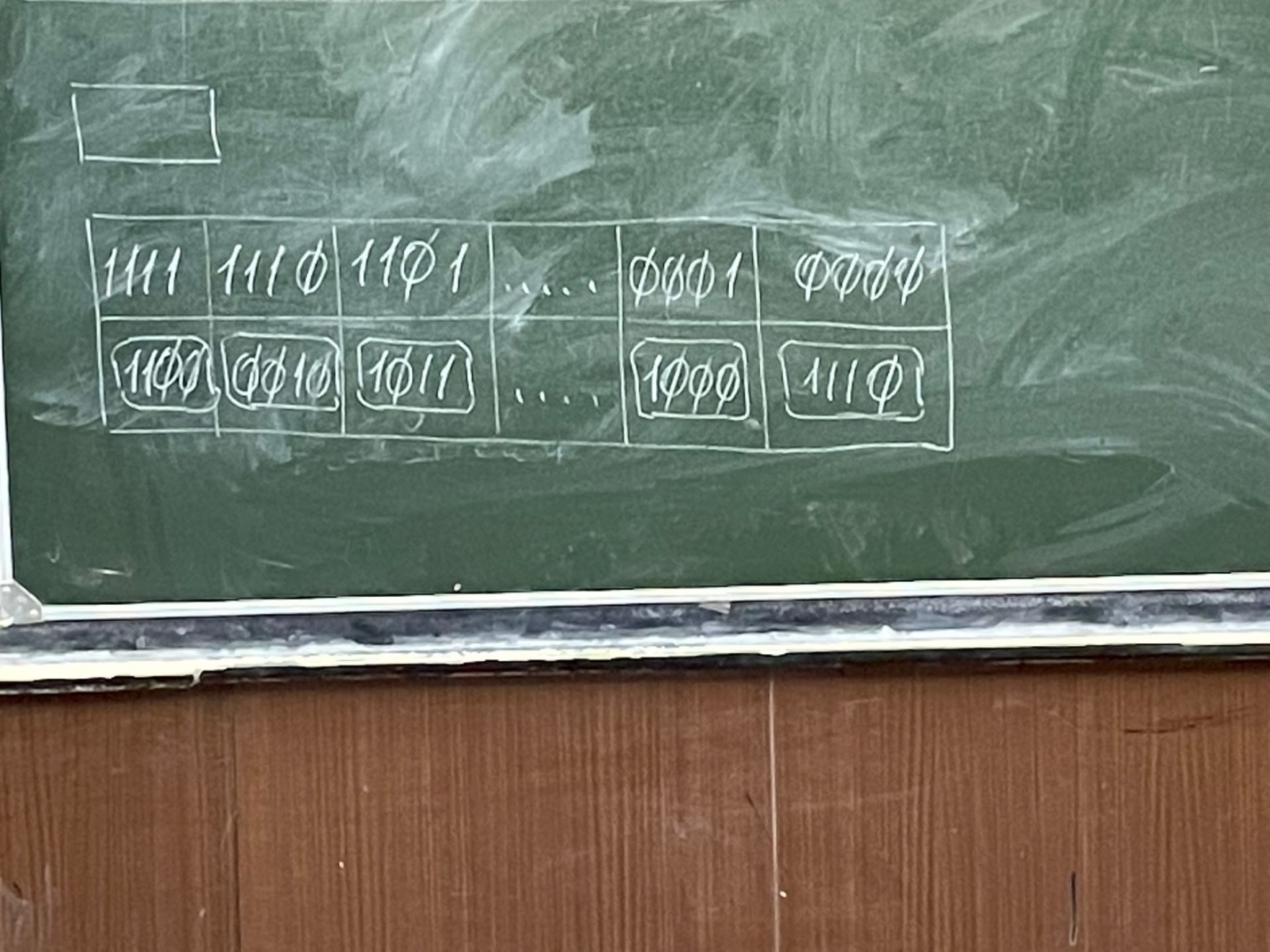
Рис. Функционировае s-блока подстановки гост

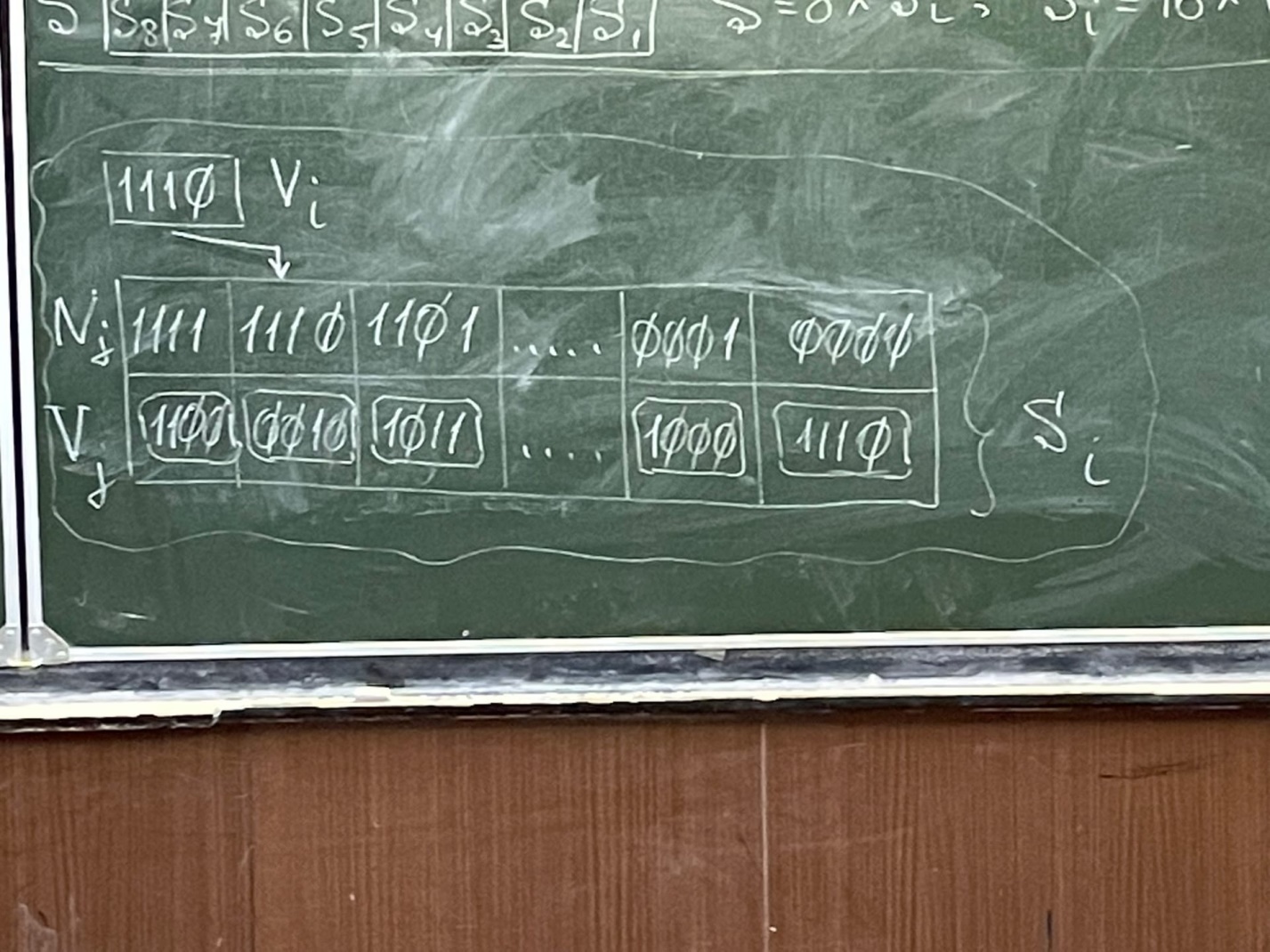


Каждый 4хразрядный вектор Vi из входног 32х разрядного вектора V идущего сумматора sm1(рис схема реализ режима прост замены в гост) поступает на один из 8 64разр субблоков подстановки блока подстановки s, кот имеет общ размер 512 бит.

Субблок подстановки si сост из 16 4разр векторов подстановки и представляет собой таблицу векторов каждому из кот присв свой …………………. В процессt замены происх замена входного вектора vi на vj порядковый номер nj которого в в таблице подстановки s с чем-то совпадает vi - vj…………………………………………………………. Замена каждого из векторов vi происходит аналогично.

Пример функционирования субблоков(таблицы) si подстановки блока подстановки s показан ниже:





Функционирование блока подстановки s

2) Циклический сдвиг влево на 11 раз-в 32-разрядного вектора, полученного с выхода блока подстановки s. Циклический сдвиг выполняется регистром сдвига r. Затем рез-т работы ф-ции шифр-я f суммируется поразрядно mod 2 сумматоре sm2 с 32-разр начальным заполнением bo накопителя n2. Затем получ на выходе sm2 результат (значение a1) записывается в накопитель n1, а старое значение переписывается в нак-ль n2(b1=a0), 1-ый цикл завершается. Последующие циклы осущ-ся аналогично при это во 2 цикле из кзу считывают зап-е х1 подключ к1, во втором цикле подключ к2 и тд…. В циклах с 9—16, а так же 17-24\*, считываются в том же порядке. В след 8 циклах 25-32 порядок считывания подключей из кзу обратный к7к6к5…к1к0, ТО при шифровании в 32 циклах осущ следующий порядок выбора из кзу подключей.

..

В 32 цикле рез-т из сумматора …

Полученный после 32 цикла шифрования заполнения накопителя n1 и n2 … соответствующих блоку открытых данных То->Tш, уравнения