Весь стандарт **ГОСТ Р 34.11-2012** написан в алгоритмической форме и ориентирован на конечных разработчиков. Однако **переход от описания на уровне шагов к логико-математическому представлению**, которое типично для криптографических примитивов, позволяет:

- оценить **криптостойкость** хеш-функции Стрибог,
- выявить **уязвимости или сильные стороны** алгоритма.

AES (англ. *Advanced Encryption Standard*; также *Rijndael*, [rɛinda:l] — *рейндал*) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES.

Представление в **AES-подобной форме** даёт следующие преимущества:

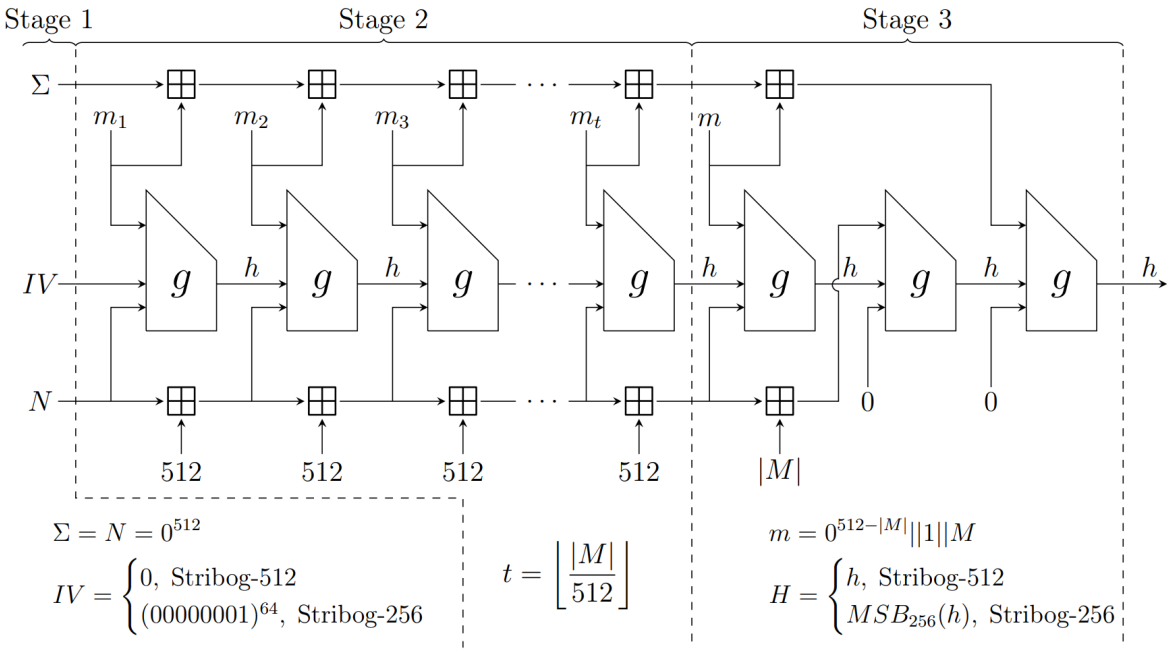
- **возможность применения известных криптоаналитических методов**, таких как дифференциальный и линейный криптоанализ;
- **возможность быстрой и эффективной реализации** с использованием таблиц и готовых техник;

Алгоритм **g_N(h, m)** внутри GOST можно переписать в **AES-подобной форме**, потому что:

  - собственный **S-бокс** → аналог AES SubBytes
  - преобразование **P** → аналог ShiftRows (только перестановка другая)
  - **линейное преобразование L** → аналог MixColumns
  - раундовые **XOR с ключом** → аналог AddRoundKey

Алгоритм хеширования состоит из **трёх стадий**:

1. **Инициализация**
2. **Итерации**
3. **Завершение**



Этапы алгоритма

1. **Инициализация**:
    - `h = IV`
        - `IV = 0x00...00` для 512 бит
        - `IV = 0x01...01` для 256 бит
    - `N = 0` — счётчик длины
    - `Σ = 0` — сумма
2. **Итерации**:

    `M` разбивается на блоки по 512 бит (`m₁, m₂, ..., m`)

    для каждого блока применяется **функция сжатия** `g_N(h, m)`
3. **Окончательная обработка**:
4. **Выходной хеш**:

- Stribog-512: `H = h`
- Stribog-256: `H = MSB₂₅₆(h)` — только старшие 256 бит

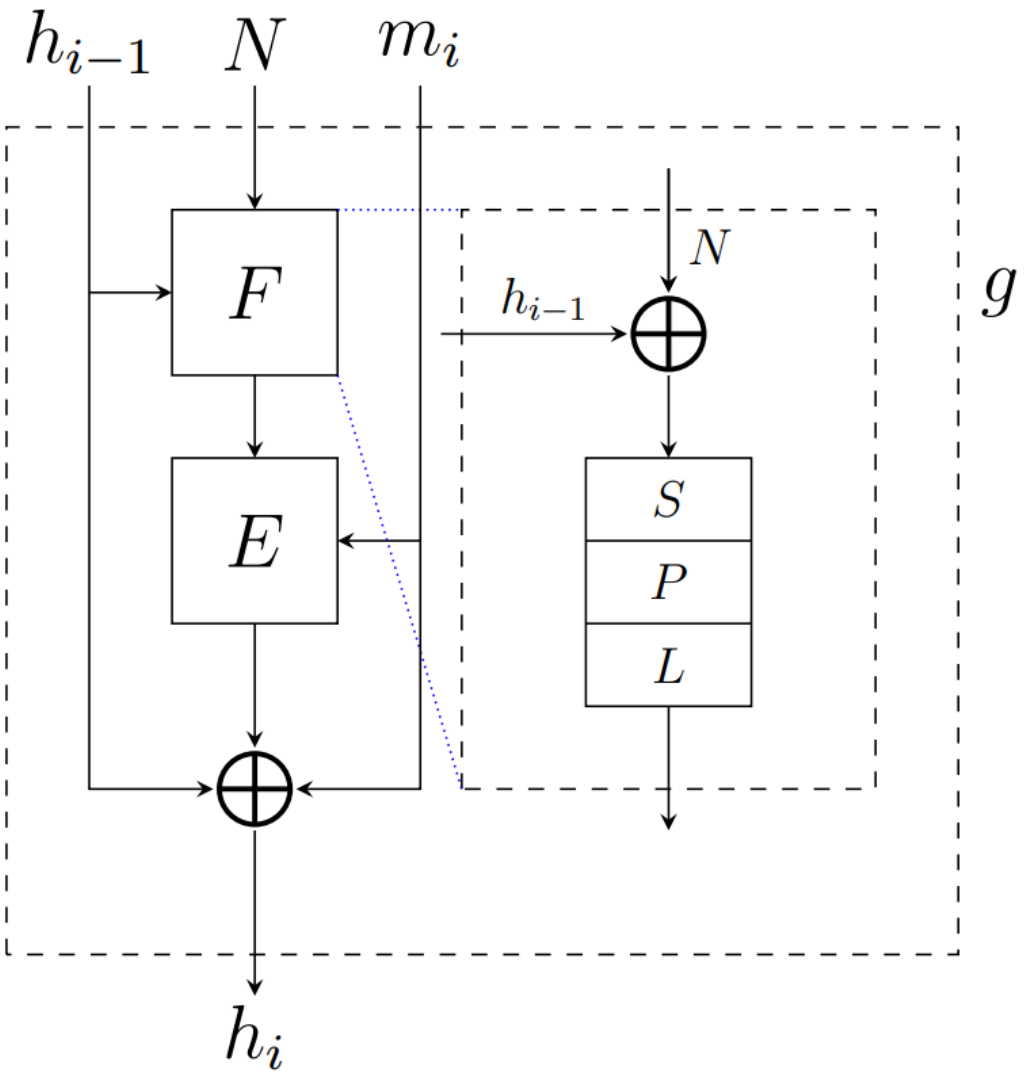
Стандарт определяет три основные трансформации, применяемые внутри функции `g_N(h, m)`:

1. **S (SubBytes)** – байтовая подстановка (аналог AES S-box)
2. **P (Permutation)** – перестановка байтов
3. **L (Linear transformation)** – линейная трансформация (аналог MixColumns)

Функция сжатия `g_N(h, m)`:

$$gN(h,m)=\mathbf{E(L\circ P\circ S(h\oplus N),m)}\oplus h\oplus m$$

- E — блочный шифр, состоящий из 12 раундов и финального шага.
- S, P, L применяются в каждом раунде, аналогично структуре AES.
- Внутреннее состояние представляется в виде **матрицы 8×8 байт** (в отличие от 4×4 в AES).



Блочный шифр E

Функция `E(K, m)` — это блочный шифр, который используется в компрессионной функции `g_N(h, m)`. Он состоит из 12 раундов и одного завершающего шага:

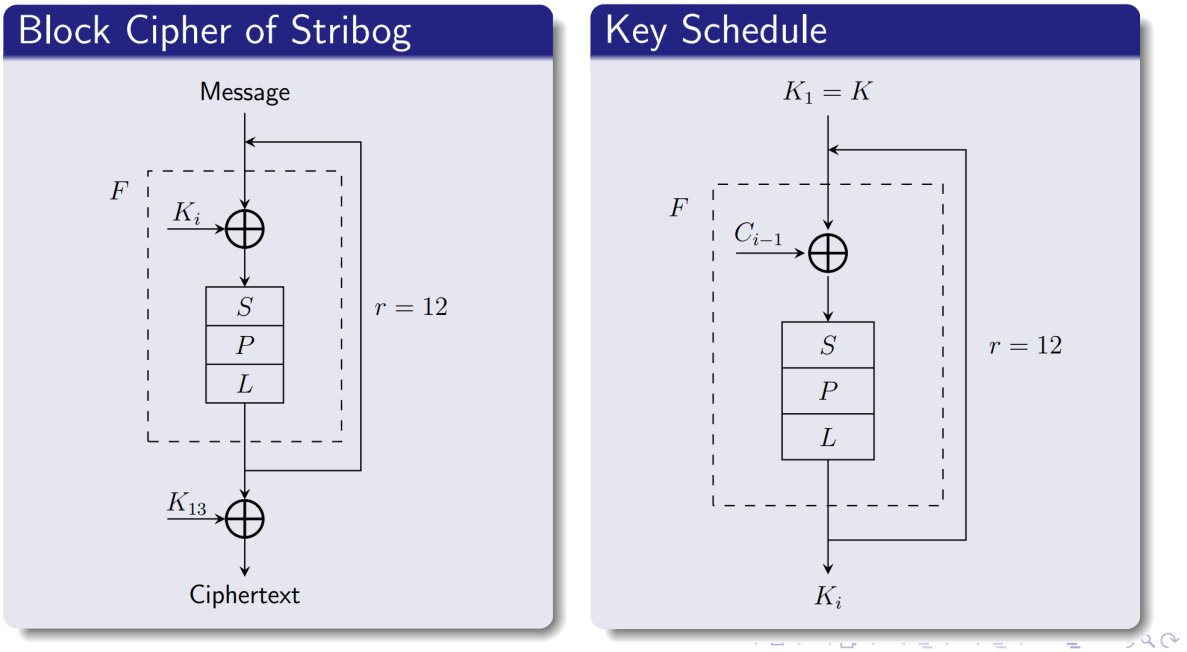
E(K,m)=X[K13]∘(L∘P∘S∘X[K12])∘...∘(L∘P∘S∘X[K1])E(K, m) = X[K₁₃] ∘ (L ∘ P ∘ S ∘ X[K₁₂]) ∘ ... ∘ (L ∘ P ∘ S ∘ X[K₁]) E(K,m)=X[K13]∘(L∘P∘S∘X[K12])∘...∘(L∘P∘S∘X[K1])

Где:

- `X[K]` — XOR с раундовым ключом (AddRoundKey)
- `K₁...K₁₃` — раундовые ключи

- $K_1 = K$ — исходный ключ
- $K_i = L \circ P \circ S(K_{i-1} \oplus C_{i-1})$ — процедура генерации ключей

Константы C_i — заранее определённые 512-битные значения



S-преобразование выполняется по аналогии с AES: каждая ячейка байтовой матрицы заменяется по таблице. S-бокс отличается от AES.

P-перестановка в Стрибоге — это не сдвиг строк, как в AES, а выполняется **транспонирование матрицы** по фиксированной перестановке τ.

L- линейное преобразование, аналогичное MixColumns в AES. Оно делается по формуле:

$$B=A \cdot M$$

Где:

- A — входной вектор (матрица состояния)
- M — фиксированная матрица 64×64 над полем $\mathbf{F}_2$

Выполняется так:

1. Разбиваем сообщение на 64-битные вектора.

2. Для каждого применяем линейное преобразование `l`, заданное матрицей.

3. Склеиваем результат обратно в байтовый вектор.

Стрибог использует **внутренний блочный шифр**, вдохновлённый **AES**, но у этих алгоритмов **разное представление данных в блоке**:

- **AES** обрабатывает данные в **матрице 4×4 байта** (128 бит), где байты идут **построчно**.

- **Стрибог** работает с блоками **512 бит (64 байта)**, но они хранятся и обрабатываются **в другом порядке**, часто **в обратном** (байты и биты читаются справа налево или снизу вверх, в зависимости от реализации).

Поскольку представления состояний в AES и Стрибог различны, сначала необходимо **обратить порядок битов** (реверсировать сообщение):

1. **R** — операция, которая обращает порядок битов входного сообщения.

    1. Свойство: $R^{-1} \circ R(x) = x$

2. Тогда компрессионная функция `g_N(h, m)` в AES-подобной форме выполняется в 3 шага:

    1. **Обращение входных битов**: `R(m)`

    2. **AES-подобные преобразования**: `S`, `P`, `L`, `X[K]`

    3. **Обратное обращение**: `R(output)`

Чтобы перейти к AES-подобной форме, все основные преобразования (`S`, `P`, `L`, `X[K]`) адаптируются следующим образом:

`S` (SubBytes)

- Применяется преобразование:
  $F'(x)=R \circ F \circ R(x) F'(x) = R \circ F \circ R(x)$ $F'(x)=R \circ F \circ R(x)$
  где `F` — оригинальный S-бокс Стрибога.

- `F'` и `F` — аффинно эквивалентны (имеют те же криптосвойства).

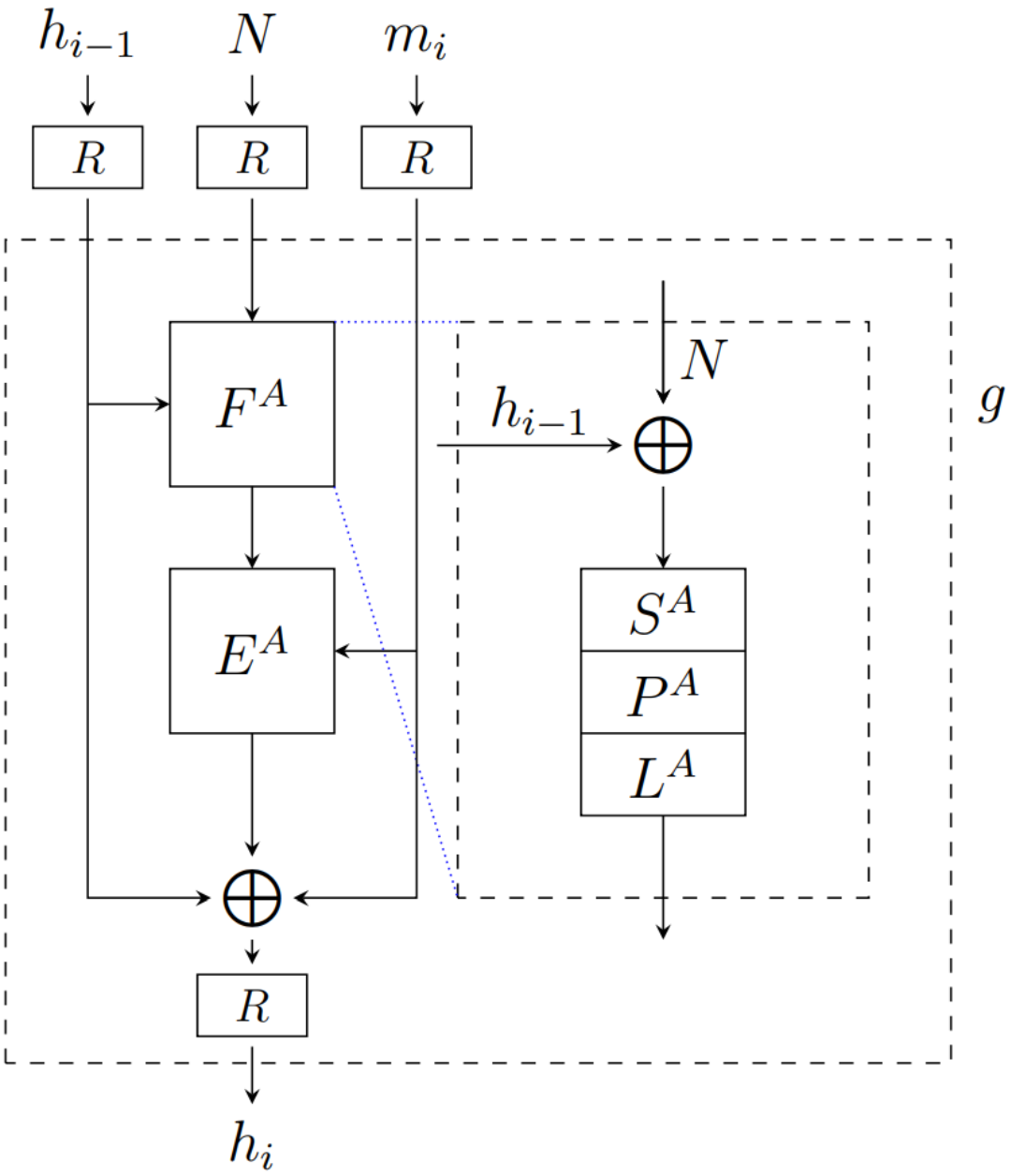
- Новый S-бокс для AES-подобной формы

`P` (Permutation) и `X[K]` (XOR с ключом)

- Работают по тем же правилам, но внутри R-обёртки.

L (Linear Transformation)

- Можно выразить как матричное умножение над конечным полем $\mathbf{F}_{2^8}$, аналогично MixColumns в AES.



$gN(h,m)=R\circ(E_K(R(m))\oplus R(h)\oplus R(m))$
https://github.com/okazymyrov/stribog

Table 3: Comparison of Stribog and AES Substitutions

Properties	Stribog	AES
Vectorial Boolean Function		
Balancedness	True	True
Nonlinearity	100	112
Absolute Indicator	96	32
Sum-of-squares Indicator	258688	133120
Propogation Criterion	0	0
Correlation Immunity	0	0
Minimum of Algebraic Degree	7	7
Resiliency	0	0
Strict Avalanche Criterion	False	False
Substitution		
Bijection	True	True
Maximum of Differential Table	8	4
Maximum of Approximation Table	28	16
Cycles Structure	252:243, 46:13	43:27, 242:87, 99:59, 124:81, 143:2
Algebraic Immunity	3(441)	2(39)