# О возможности модификации алгоритма шифрования ГОСТ 28147-89 с сохранением приемлемых эксплуатационных характеристик

Андрей Дмух  Денис Дыгин  Григорий Маршалко

2 апреля 2013 г.

## Алгоритм ГОСТ 28147-89

- Более 20 лет (до 2011 года) не было снижения стойкости

## Алгоритм ГОСТ 28147-89

- Более 20 лет (до 2011 года) не было снижения стойкости
- Метод Исобе: $2^{225}$ операций зашифрования на $2^{32}$ парах открытого - шифрованного текста

## Алгоритм ГОСТ 28147-89

- Более 20 лет (до 2011 года) не было снижения стойкости
- Метод Исобе: $2^{225}$ операций зашифрования на $2^{32}$ парах открытого - шифрованного текста
- Метод Динура-Данкельмана-Шамира: $2^{192}$ операций зашифрования на $2^{64}$ парах открытого - шифрованного текста

## Алгоритм ГОСТ 28147-89

- Более 20 лет (до 2011 года) не было снижения стойкости
- Метод Исобе: $2^{225}$ операций зашифрования на $2^{32}$ парах открытого - шифрованного текста
- Метод Динура-Данкельмана-Шамира: $2^{192}$ операций зашифрования на $2^{64}$ парах открытого - шифрованного текста

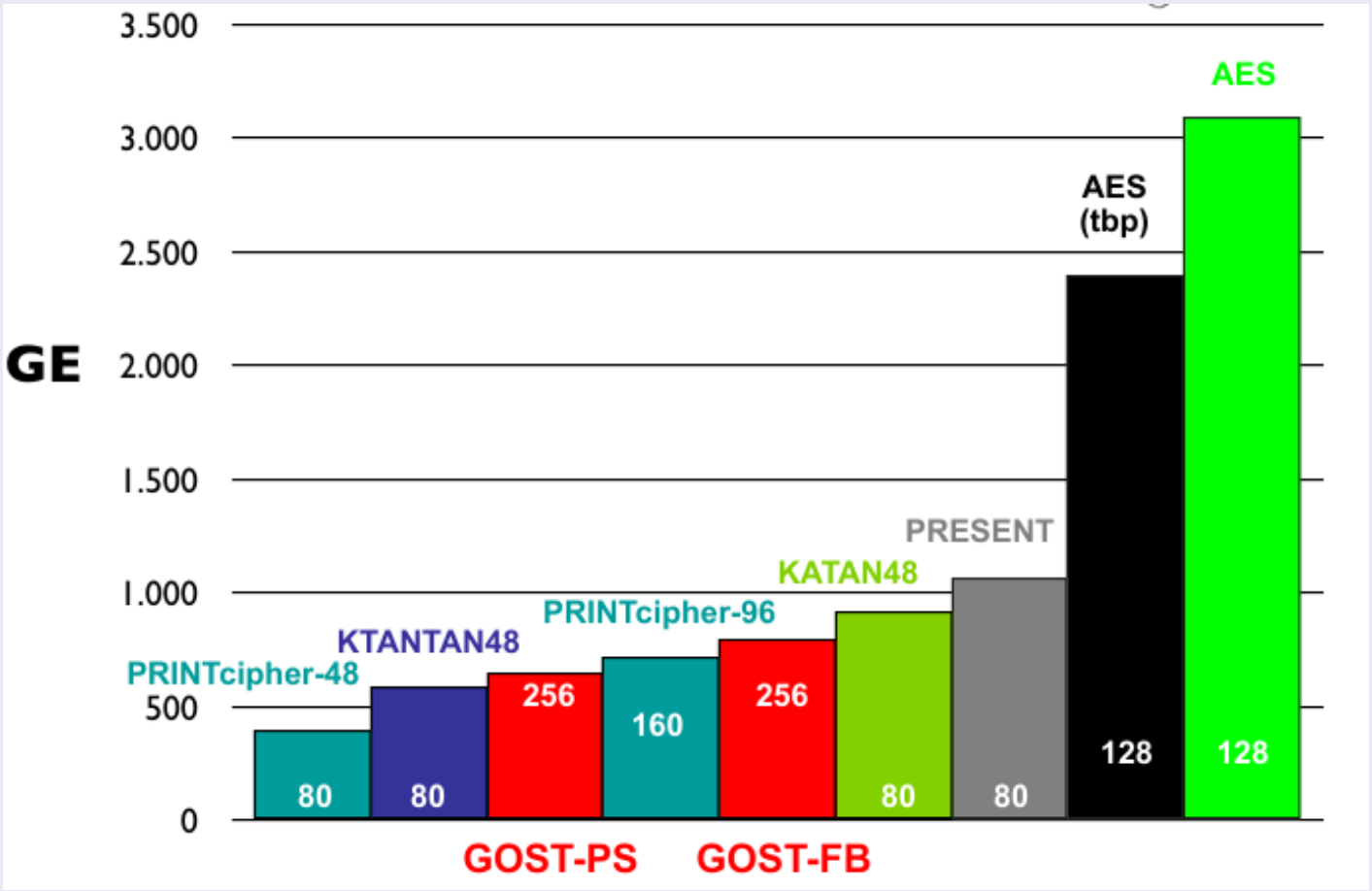
- $2^{192}$ нереализуемо

## Алгоритм ГОСТ 28147-89

- Более 20 лет (до 2011 года) не было снижения стойкости
- Метод Исобе: $2^{225}$ операций зашифрования на $2^{32}$ парах открытого - шифрованного текста
- Метод Динура-Данкельмана-Шамира: $2^{192}$ операций зашифрования на $2^{64}$ парах открытого - шифрованного текста

- $2^{192}$ нереализуемо
- На материале $2^{\frac{n}{2}}$ блочный шифр с длиной блока $n$ бит, считается нестойким – парадокс дней рождения (ISO/IEC JTC 1/SC 27 Standing Document 12)

# ГОСТ 28147-89 крайне удачен с точки зрения lightweight-реализации



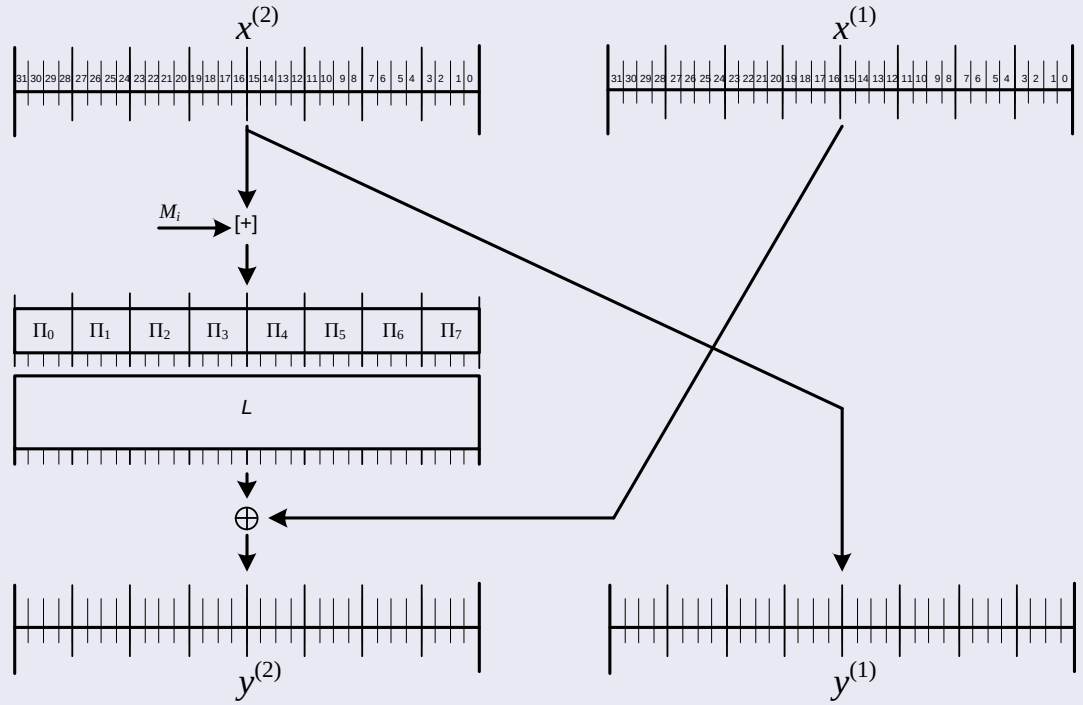

Данные об эффективности реализации различных криптографических алгоритмов (A. Poschmann, S. Ling, H. Wang 2010)

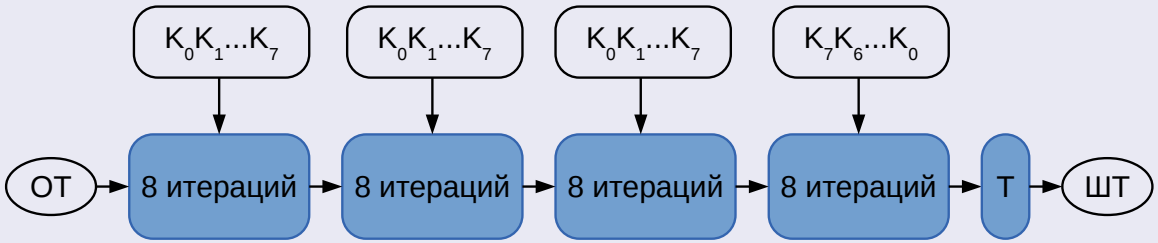
Можно ли модифицировать алгоритм таким образом, чтобы сохранив достоинства эффективной lightweight-реализации, исключить возможность применения методов Исобе и Динура-Данкельмана-Шамира?

Можно ли модифицировать алгоритм таким образом, чтобы сохранив достоинства эффективной lightweight-реализации, исключить возможность применения методов Исобе и Динура-Данкельмана-Шамира?

Определяющее свойство – простота ключевой развертки

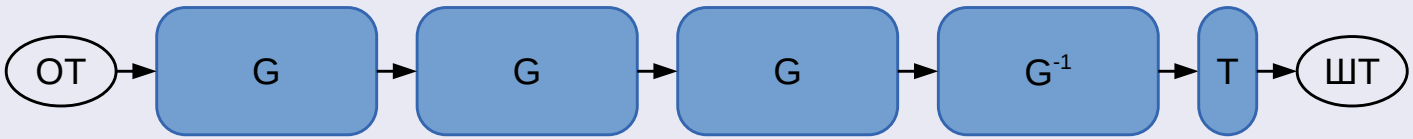
# Схематичное описание алгоритма (базовая итерация)



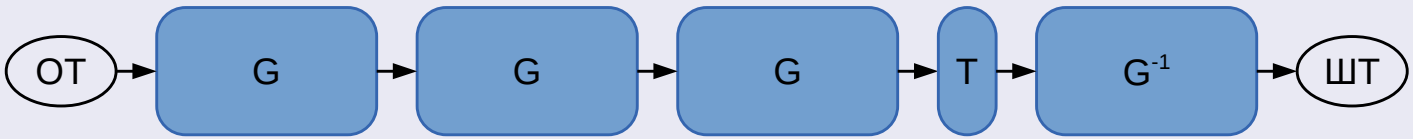
# Метод Исобе

- Зашифрование блока ОТ представимо в виде $CT = G \cdot G \cdot G \cdot G^{-1} \cdot T(OT)$, $G$ – 8 итераций с ключами $K_7 K_6 \ldots K_0$



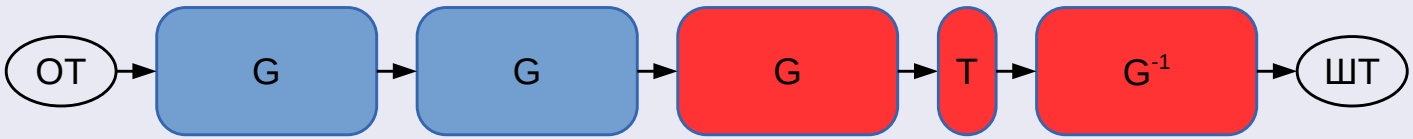
# Метод Исобе

- Зашифрование блока ОТ представимо в виде $CT = G \cdot G \cdot G \cdot G^{-1} \cdot T(OT)$, $G$ – 8 итераций с ключами $K_7 K_6 \ldots K_0$
- $T$ – перестановочно с $G$, $CT = G \cdot G \cdot G \cdot T \cdot G^{-1}(OT)$



# Метод Исобе

- Зашифрование блока ОТ представимо в виде $CT = G \cdot G \cdot G \cdot G^{-1} \cdot T(OT)$, $G$ – 8 итераций с ключами $K_7 K_6 \ldots K_0$
- $T$ – перестановочно с $G$, $CT = G \cdot G \cdot G \cdot T \cdot G^{-1}(OT)$
- С вероятностью $2^{-32}$ существует фиксированная точка



## Метод Исобе

- Зашифрование блока ОТ представимо в виде $CT = G \cdot G \cdot G \cdot G^{-1} \cdot T(OT)$, $G$ – 8 итераций с ключами $K_7 K_6 \ldots K_0$
- $T$ – перестановочно с $G$, $CT = G \cdot G \cdot G \cdot T \cdot G^{-1}(OT)$
- С вероятностью $2^{-32}$ существует фиксированная точка
- Метод встречи посередине

Общая трудоемкость метода Исобе составляет $2^{225}$ операций зашифрования при необходимом материале $2^{32}$ известных пар открытого-шифрованного текста с вероятностью успеха $0,63$.

## Метод Динура-Данкельмана-Шамира

Два подхода, развивающие метод Исобе: метод встречи посередине не для одной пары открытого-шифрованного текста 16 итерациях, как в методе Исобе, а для двух пар открытого-шифрованного текста на 8 итерациях

## Метод Динура-Данкельмана-Шамира

Два подхода, развивающие метод Исобе: метод встречи посередине не для одной пары открытого-шифрованного текста 16 итерациях, как в методе Исобе, а для двух пар открытого-шифрованного текста на 8 итерациях

- Трудоемкость первого подхода составляет $1,5 \cdot 2^{192}$ операций зашифрования при необходимом материале $2^{64}$ известных пар открытого-шифрованного текста с вероятностью успеха $0,63$.

## Метод Динура-Данкельмана-Шамира

Два подхода, развивающие метод Исобе: метод встречи посередине не для одной пары открытого-шифрованного текста 16 итерациях, как в методе Исобе, а для двух пар открытого-шифрованного текста на 8 итерациях

- Трудоемкость первого подхода составляет $1,5 \cdot 2^{192}$ операций зашифрования при необходимом материале $2^{64}$ известных пар открытого-шифрованного текста с вероятностью успеха $0,63$.
- Трудоемкость второго подхода – $1,5 \cdot 2^{224}$ операций зашифрования, материал $2^{32}$ известных пар открытого-шифрованного текста, вероятность успеха $0,63$.

## Идея модификации

- Изменением ключевой развертки уменьшить вероятности выполнения свойства отражения и появления неподвижных точек

## Идея модификации

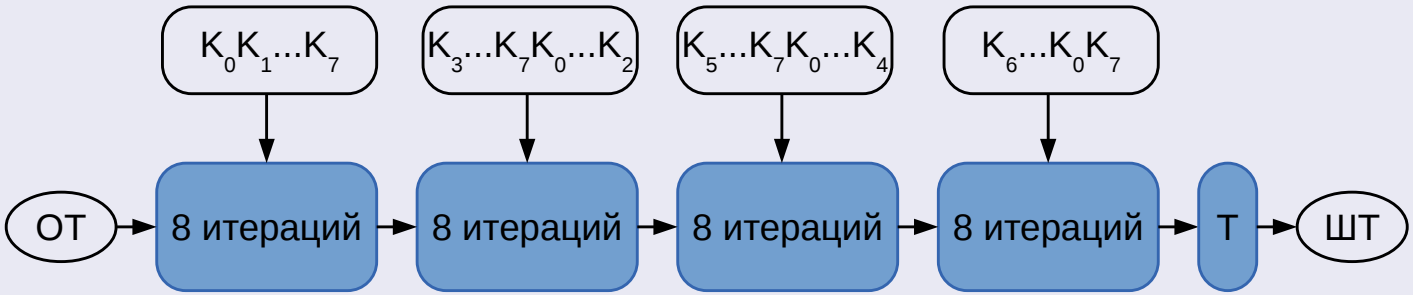
- Изменением ключевой развертки уменьшить вероятности выполнения свойства отражения и появления неподвижных точек
- Использовать два нелинейных элемента-подстановки, с тем, чтобы 'не складывать яйца в одну корзину', но не сильно усложнять аппаратную реализацию

## Идея модификации

- Изменением ключевой развертки уменьшить вероятности выполнения свойства отражения и появления неподвижных точек
- Использовать два нелинейных элемента-подстановки, с тем, чтобы 'не складывать яйца в одну корзину', но не сильно усложнять аппаратную реализацию
- Зафиксировать конкретные подстановки, чтобы избежать некорректных выводов о свойствах алгоритма (Куртуа)

# 2-ГОСТ – модификация алгоритма ГОСТ 28147-89

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | $K_0$ | $K_1$ | $K_2$ | $K_3$ | $K_4$ | $K_5$ | $K_6$ | $K_7$ |
| 1 | $K_3$ | $K_4$ | $K_5$ | $K_6$ | $K_7$ | $K_0$ | $K_1$ | $K_2$ |
| 2 | $K_5$ | $K_6$ | $K_7$ | $K_0$ | $K_1$ | $K_2$ | $K_3$ | $K_4$ |
| 3 | $K_6$ | $K_5$ | $K_4$ | $K_3$ | $K_2$ | $K_1$ | $K_0$ | $K_7$ |



## Фиксированный набор подстановок

- $\pi_0 = \pi_1 = \pi_2 = \pi_3 = \pi_1$ , где
  $\pi_1 = (6,A,F,4,3,8,5,0,D,E,7,1,2,B,C,9)$
- $\pi_4 = \pi_5 = \pi_6 = \pi_7 = \pi_2$ , где
  $\pi_2 = (E,0,8,1,7,A,5,6,D,2,4,9,3,F,C,B)$

## Возможность применения описанных атак

- Для модифицированного алгоритма ГОСТ вероятность выполнения свойства отражения в методе Исобе равна
$P\{K_0 = K_2 = K_4 = K_6, K_1 = K_3 = K_5 = K_7\} = 2^{-192}$
(при условии случайного равновероятного распределения на множестве всех ключей), то есть пренебрежимо мала

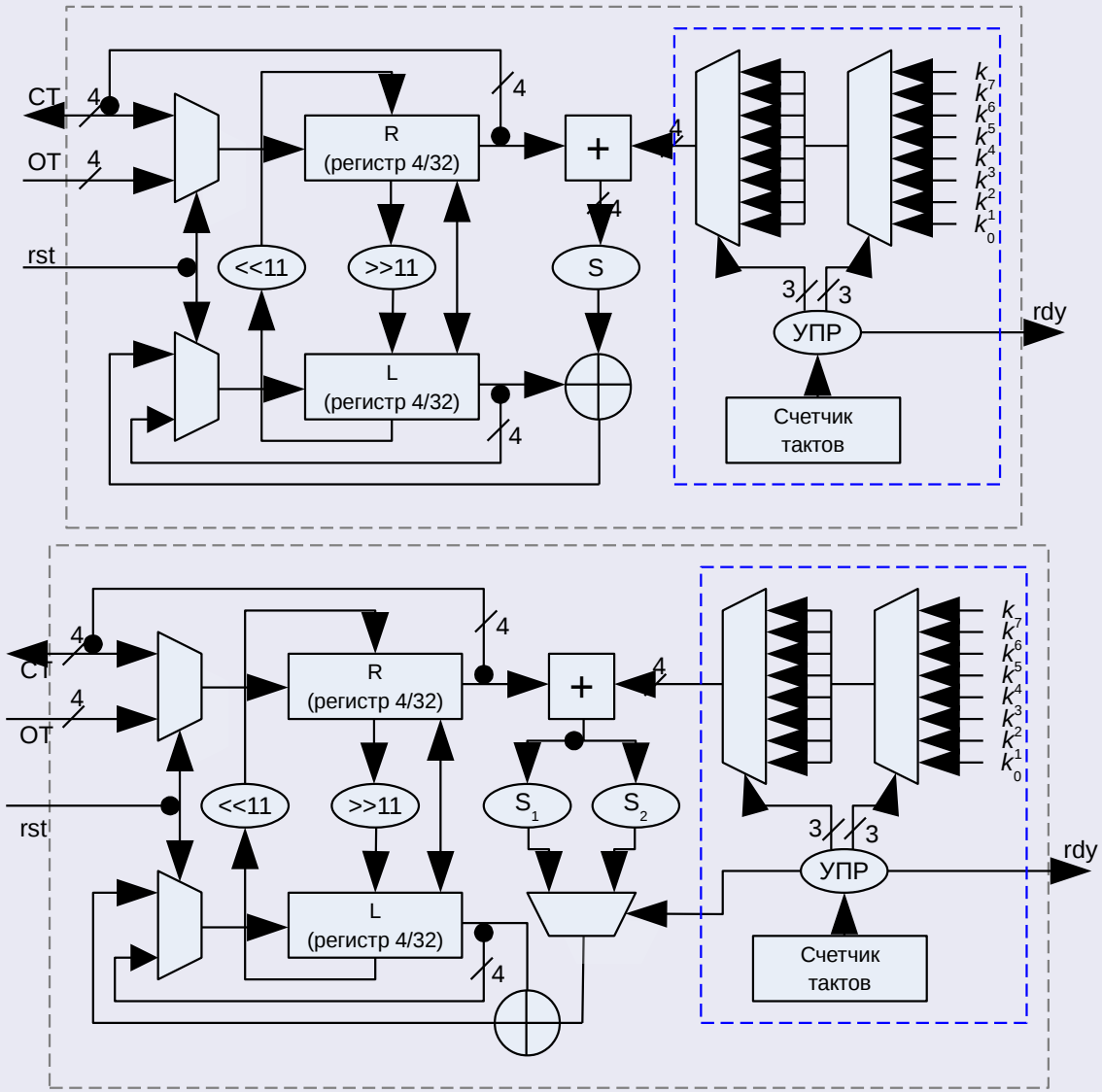
## Возможность применения описанных атак

- Для модифицированного алгоритма ГОСТ вероятность выполнения свойства отражения в методе Исобе равна
  $P\{K_0 = K_2 = K_4 = K_6, K_1 = K_3 = K_5 = K_7\} = 2^{-192}$
  (при условии случайного равновероятного распределения на множестве всех ключей), то есть пренебрежимо мала
- В первом методе Динура, Данкельмана и Шамира необходимо выполнение равенств
  $K_0 = K_2 = K_4 = K_6 = K_1 = K_3 = K_5 = K_7$. Вероятность этого события равна $2^{-224}$.

## Возможность применения описанных атак

- Для модифицированного алгоритма ГОСТ вероятность выполнения свойства отражения в методе Исобе равна $P\{K_0 = K_2 = K_4 = K_6, K_1 = K_3 = K_5 = K_7\} = 2^{-192}$ (при условии случайного равновероятного распределения на множестве всех ключей), то есть пренебрежимо мала
- В первом методе Динура, Данкельмана и Шамира необходимо выполнение равенств $K_0 = K_2 = K_4 = K_6 = K_1 = K_3 = K_5 = K_7$. Вероятность этого события равна $2^{-224}$.
- Простота ключевой развертки – возможность применения методов связанных ключей, которые однако труднореализуемы на практике (Рудской, 2011)

# Аппаратные реализации исходного и модифицированного алгоритмов



## Аппаратная реализация алгоритма

- Выбор итерационного ключа в исходном алгоритме может быть организован с помощью 3-битного и 2-битного счетчиков, выбор 4-битного подключа – с помощью еще одного 3-битного счетчика.

## Аппаратная реализация алгоритма

- Выбор итерационного ключа в исходном алгоритме может быть организован с помощью 3-битного и 2-битного счетчиков, выбор 4-битного подключа – с помощью еще одного 3-битного счетчика.
- В модифицированном алгоритме номер ключа может быть вычислен с помощью первых двух счетчиков дополнительной ROM памяти (4 блока по 3 бита) и сумматора на 3 бита.

## Аппаратная реализация алгоритма

- Выбор итерационного ключа в исходном алгоритме может быть организован с помощью 3-битного и 2-битного счетчиков, выбор 4-битного подключа – с помощью еще одного 3-битного счетчика.
- В модифицированном алгоритме номер ключа может быть вычислен с помощью первых двух счетчиков дополнительной ROM памяти (4 блока по 3 бита) и сумматора на 3 бита.
- При реализации на ПЛИС подстановка реализуется в виде блока ячеек (16 слов по 4 бита) и независит от конретного вида подстановки. Для двух подстановок – 2 блока памяти и мультиплексор, зависящий от исходных счетчиков.

## Оценка сложности реализации изменений для ПЛИС

Предложенные модификации увеличивают оценку GE

- менее 2% для внешне задаваемого ключа
- менее 6% для фиксированного ключа

## Оценка сложности реализации изменений для ПЛИС

Предложенные модификации увеличивают оценку GE

- менее 2% для внешне задаваемого ключа
- менее 6% для фиксированного ключа

## Оценка сложности реализации изменений для СБИС

- Дополнительная подстановка – не более 30 GE
- Дополнительный 3-х битный счетчик – 23 GE
- Демультиплексор – не более 15 GE

Всего – не более 750 GE

| | САПР Xilinx ISE 9.2 | САПР Xilinx ISE 9.2 | САПР Synopsys DesignCompiler |
|---|---|---|---|
| | внешний ключ | фиксированный ключ | фиксированный ключ |
| ГОСТ 28147-89 | 2137 GE | 1556 GE | 650GE |
| 2-ГОСТ | 2158 GE | 1570 GE | ≈750 GE |

Спасибо за внимание