Обзор последних публикаций по криптографическим исследованиям алгоритма шифрования ГОСТ 28147-89

В.И. Рудской
rudskoy_vladimir@mail.ru

ФСБ России

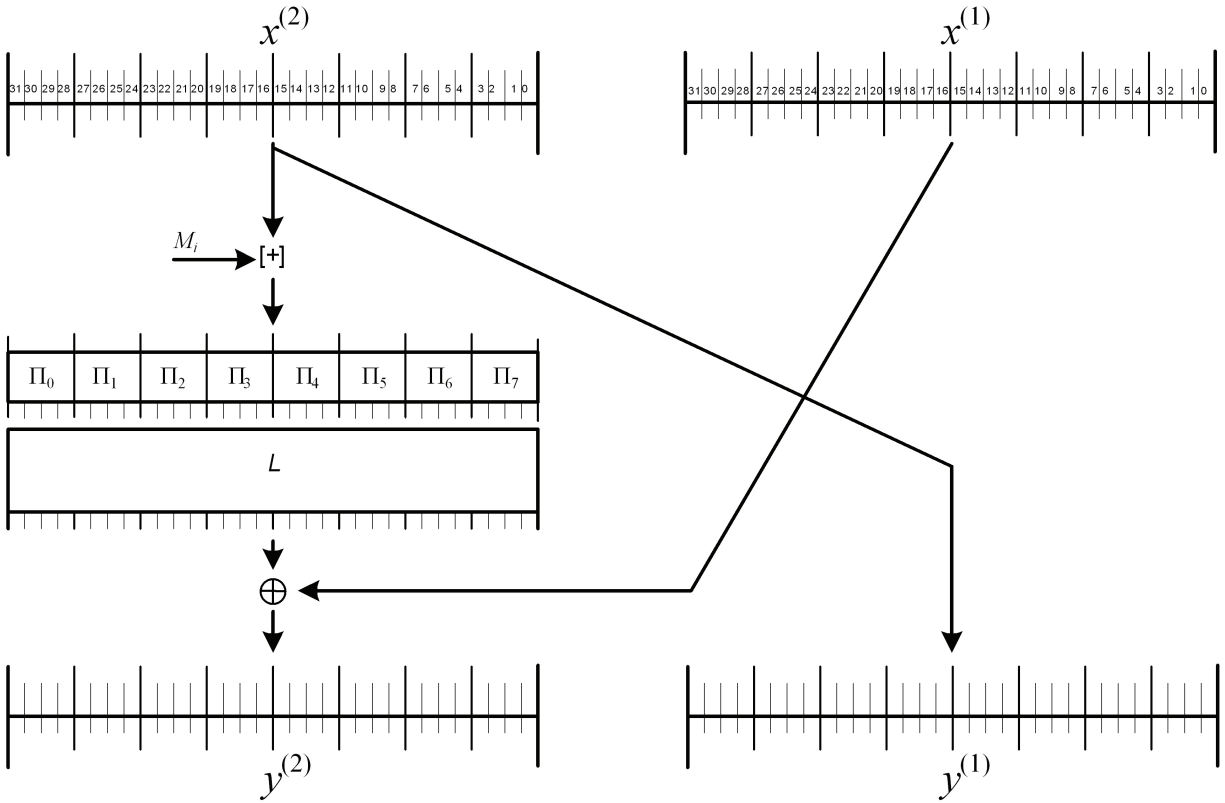
XIV международная конференция «РусКрипто'2012»

Публикации по криптоанализу алгоритма ГОСТ 28147-89

1. Основные результаты
   - O. Kara – «Reflection Attacks on Product Ciphers» (INDOCRYPT 2008)
   - T. Isobe – «A Single-Key Attack on the Full GOST Block Cipher» (FSE 2011, JoC)
   - I. Dinur, O. Dunkelman, A. Shamir – «Improved Attacks on Full GOST» (ePrint, FSE 2012)
   - Bo Zhu, Guang Gong – «Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2»

2. Другие «результаты»
   - N. Courtois – «Algebraic Complexity Reduction and Cryptanalysis of GOST», и еще не менее 3 работ
   - N. Courtois, M. Misztal – «Differential Cryptanalysis of GOST», и еще не менее 2 работ

Описание алгоритма ГОСТ 28147-89



Ключевая развертка:

$$[K_1, K_2, ..., K_8], [K_1, ..., K_8], [K_1, ..., K_8], [K_8, ..., K_1]$$

Публикации по криптоанализу алгоритма ГОСТ 28147-89

1. Основные результаты
   - O. Kara – «Reflection Attacks on Product Ciphers» (INDOCRYPT 2008)
   - T. Isobe – «A Single-Key Attack on the Full GOST Block Cipher» (FSE 2011, JoC)
   - I. Dinur, O. Dunkelman, A. Shamir – «Improved Attacks on Full GOST» (ePrint, FSE 2012)
   - Bo Zhu, Guang Gong – «Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2»

2. Другие «результаты»
   - N. Courtois – «Algebraic Complexity Reduction and Cryptanalysis of GOST», и еще не менее 3 работ
   - N. Courtois, M. Misztal – «Differential Cryptanalysis of GOST», и еще не менее 2 работ

Reflection property

- $H = F \circ G \circ F^{-1}$
- $G(x) = x$
- $y = F^{-1}(x)$
- $H(y) = y$

Применение к ГОСТ 28147-89

- $E_K = F_K \circ F_K \circ F_K \circ S \circ F_K^{-1}$
- S имеет 2^{32} неподвижных точек
- $E_K(x) = y \quad \Rightarrow \quad F_K^2(x) = y$

Reflection property

- $H = F \circ G \circ F^{-1}$
- $G(x) = x$
- $y = F^{-1}(x)$
- $H(y) = y$

Применение к ГОСТ 28147-89

- $E_K = F_K \circ F_K \circ F_K \circ S \circ F_K^{-1}$
- S имеет 2^{32} неподвижных точек
- $E_K(x) = y \quad \Rightarrow \quad F_K^2(x) = y$

Слабые ключи

- $F_K(x) = x$ и $S(x) = x$
- $E_K(x) = x$
- Решение $F_K(x) = x$: перебор $k_1, ..., k_6$, вычисление k_7, k_8
- Трудоемкость 2^{192}
- Материал 2^{32} подобранных открытых текстов
- Доля ключей 2^{-32}

Усечение до 30 итераций (без первых двух)

- $F_K[3, 8] \circ F_K[1, 8](x) = y$
- Перебор $k_3, ..., k_8$ вычисление k_1, k_2
- Материал 2^{32} известных открытых текстов
- Трудоемкость $2^{192} \cdot 2^{32} = 2^{224}$

Слабые ключи

- $F_K(x) = x$ и $S(x) = x$
- $E_K(x) = x$
- Решение $F_K(x) = x$: перебор $k_1, ..., k_6$, вычисление k_7, k_8
- Трудоемкость 2^{192}
- Материал 2^{32} подобранных открытых текстов
- Доля ключей 2^{-32}

Усечение до 30 итераций (без первых двух)

- $F_K[3,8] \circ F_K[1,8](x) = y$
- Перебор $k_3, ..., k_8$ вычисление k_1, k_2
- Материал 2^{32} известных открытых текстов
- Трудоемкость $2^{192} \cdot 2^{32} = 2^{224}$

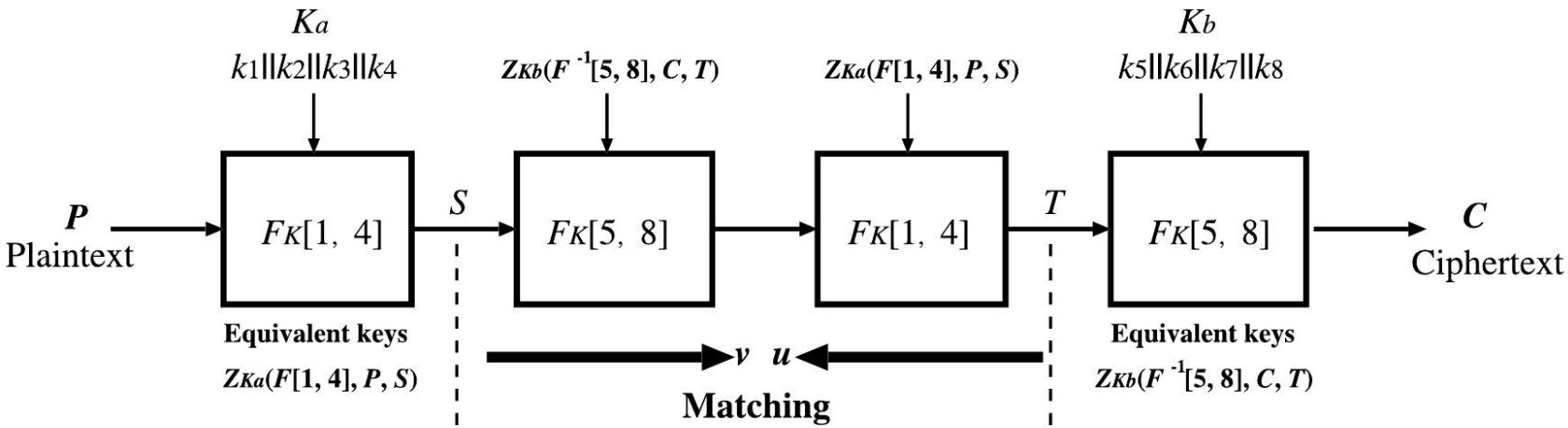
Публикации по криптоанализу алгоритма ГОСТ 28147-89

1. Основные результаты
   - O. Kara – «Reflection Attacks on Product Ciphers» (INDOCRYPT 2008)
   - T. Isobe – «A Single-Key Attack on the Full GOST Block Cipher» (FSE 2011, JoC)
   - I. Dinur, O. Dunkelman, A. Shamir – «Improved Attacks on Full GOST» (ePrint, FSE 2012)
   - Bo Zhu, Guang Gong – «Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2»

2. Другие «результаты»
   - N. Courtois – «Algebraic Complexity Reduction and Cryptanalysis of GOST», и еще не менее 3 работ
   - N. Courtois, M. Misztal – «Differential Cryptanalysis of GOST», и еще не менее 2 работ

«A Single-Key Attack on the Full GOST Block Cipher»

- Использование «Reflection property»
- Атака Meet-in-the-Middle на 16 раундов по одной паре вход-выход
- Построение множеств эквивалентных ключей для 4 раундов
- При биективных S-боксах по (P, S, k_1, k_2) вычисляются (k_3, k_4)



- Трудоемкость
  $(2^{128}(2^{64} + 2^{64}) + (2^{128} \cdot 2^{64} + 2^{128} \cdot 2^{64} \cdot 2^{-64} + \ldots)) \times 2^{32} = 2^{225}$
- Утверждается, что для произвольных S-боксов результат тот же (?!)

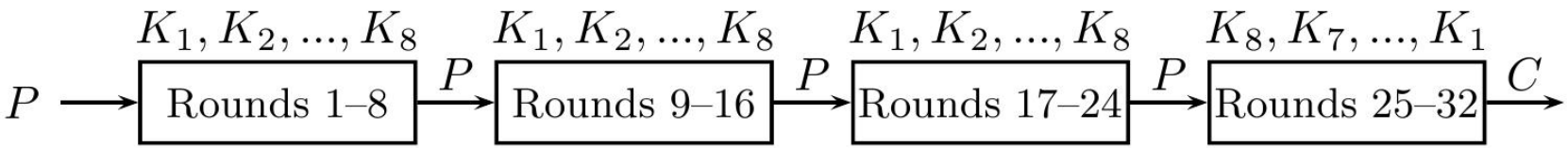
Публикации по криптоанализу алгоритма ГОСТ 28147-89

1. Основные результаты
   - O. Kara – «Reflection Attacks on Product Ciphers» (INDOCRYPT 2008)
   - T. Isobe – «A Single-Key Attack on the Full GOST Block Cipher» (FSE 2011, JoC)
   - I. Dinur, O. Dunkelman, A. Shamir – «Improved Attacks on Full GOST» (ePrint, FSE 2012)
   - Bo Zhu, Guang Gong – «Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2»
2. Другие «результаты»
   - N. Courtois – «Algebraic Complexity Reduction and Cryptanalysis of GOST», и еще не менее 3 работ
   - N. Courtois, M. Misztal – «Differential Cryptanalysis of GOST», и еще не менее 2 работ

«Improved Attacks on Full GOST»

- Атака на 8 раундов по двум парам вход-выход
- Уменьшается количество ключей прошедших фильтрацию $2^{192} \rightarrow 2^{128}$
- Пары вход-выход вычисляются с использованием «Reflection property» и с использованием неподвижных точек 8 раундов зашифрования
- В случае существования неподвижной точки 8 раундов зашифрования общая трудоемкость атаки снижается по сравнению с предыдущими работами
- Предложен алгоритм фильтрации с малыми требованиями к памяти (за счет увеличения общей трудоемкости)
- Используется слабое «рассеивание» алгоритма ГОСТ

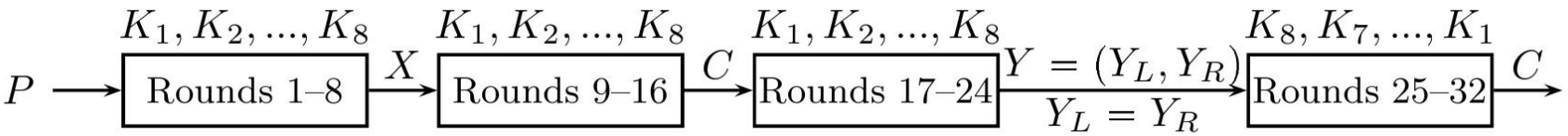
- Предполагается существование неподвижной точки $F_K(P) = P$
- Неподвижная точка не обязательно существует
- Необходимый исходный материал 2^{64}
- $E_K(P) = C$
- $F_K(P) = P$ и $F_K(C) = \overline{P}$
- Трудоемкость атаки $2^{64} \cdot \max(2^{128}, T_8) \geq 2^{192}$



«Improved Attacks on Full GOST»

«Reflection property»

- Перебор всех X – дополнительный множитель 2^{64} в трудоемкость
- Неподвижные точки для $F_K \circ S \circ F_K^{-1}$ существуют
- Исходный материал 2^{32}
- Пары (P, X) и (X, C)
- Трудоемкость атаки $2^{32} \cdot 2^{64} \cdot \max(2^{128}, T_8) \geq 2^{224}$



«Improved Attacks on Full GOST»

Атака на 8 раундов по 2 парам вход-выход

(I, O) и (I^*, O^*)

Простейшая атака MitM

- Перебор $K_1 - K_4$ и вычисление Y, Y^* по I, I^*
- Перебор $K_5 - K_8$ и вычисление $\widehat{Y}, \widehat{Y^*}$ по O, O^*
- Согласование $Y = \widehat{Y}$ и $Y^* = \widehat{Y^*}$
- Трудоемкость 2^{128}, Память 2^{128}

MitM-атака с использованием эквивалентных ключей

- Перебор Y
- Построение множества эквивалентных ключей $F_K[1,4](I) = Y$
- Вычисление для каждого ключа Y^*
- Аналогично $F_K[5,8](Y) = O$, вычисление $\widehat{Y^*}$
- согласование $Y^* = \widehat{Y^*}$
- Трудоемкость 2^{128}, Память 2^{64}

«Improved Attacks on Full GOST»

Атака на 8 раундов по 2 парам вход-выход

(I, O) и (I^*, O^*)

Простейшая атака MitM

- Перебор $K_1 - K_4$ и вычисление Y, Y^* по I, I^*
- Перебор $K_5 - K_8$ и вычисление $\widehat{Y}, \widehat{Y^*}$ по O, O^*
- Согласование $Y = \widehat{Y}$ и $Y^* = \widehat{Y^*}$
- Трудоемкость 2^{128}, Память 2^{128}

MitM-атака с использованием эквивалентных ключей

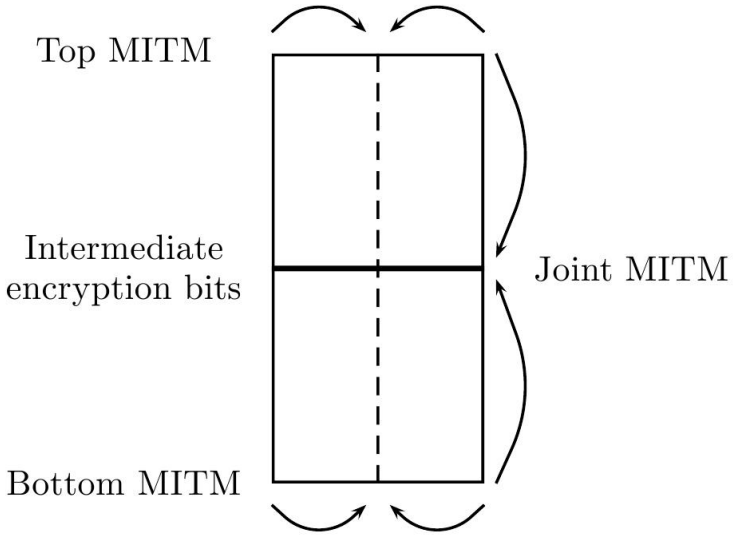
- Перебор Y
- Построение множества эквивалентных ключей $F_K[1,4](I) = Y$
- Вычисление для каждого ключа Y^*
- Аналогично $F_K[5,8](Y) = O$, вычисление $\widehat{Y^*}$
- согласование $Y^* = \widehat{Y^*}$
- Трудоемкость 2^{128}, Память 2^{64}

- Перебор ключей $K_5 - K_8$ и частичное расшифрование Y, Y^*
- Использование уравнений, связывающих вход, выход, ключ и промежуточные состояния как в работе Isobe
- Перебор/определение части бит ключа и промежуточных состояний
- Наличие двух пар вход-выход позволяет исключить неизвестные ключи: $Z \boxplus K = Q$ и $Z^* \boxplus K = Q^* \Rightarrow Z \boxminus Z^* = Q \boxminus Q^*$
- Построение дерева перебора. Обход дерева в глубину с проверкой непротиворечивости на каждом шаге
- Вычисление K_1, K_4 и промежуточных состояний с последующим вычислением K_2, K_3
- Трудоемкость 2^{140}, память 2^{19}

«Improved Attacks on Full GOST»

Использование слабого рассеивания - 2 Dimentional MitM

- Перебор части бит Y, Y^*
- Применение предыдущей атаки к первым 4 итерациям и к последним 4 итерациям
- Согласование и получение возможных ключей
- Трудоемкость 2^{128}, память 2^{36}

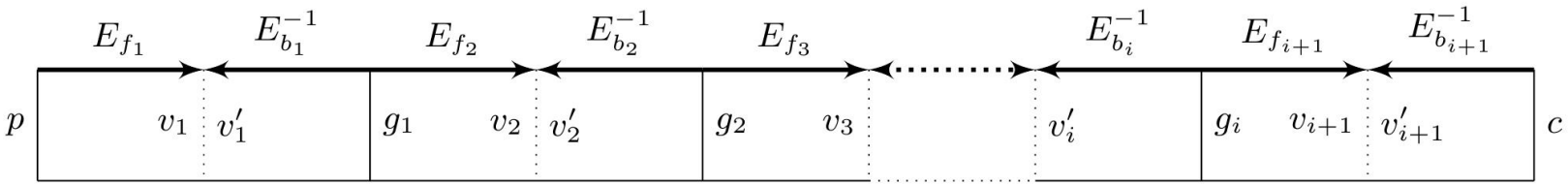


Публикации по криптоанализу алгоритма ГОСТ 28147-89

1. Основные результаты
   - O. Kara – «Reflection Attacks on Product Ciphers» (INDOCRYPT 2008)
   - T. Isobe – «A Single-Key Attack on the Full GOST Block Cipher» (FSE 2011, JoC)
   - I. Dinur, O. Dunkelman, A. Shamir – «Improved Attacks on Full GOST» (ePrint, FSE 2012)
   - **Bo Zhu, Guang Gong – «Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2»**
2. Другие «результаты»
   - N. Courtois – «Algebraic Complexity Reduction and Cryptanalysis of GOST», и еще не менее 3 работ
   - N. Courtois, M. Misztal – «Differential Cryptanalysis of GOST», и еще не менее 2 работ

«Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2»

- Разбиение на 4 интервала:
  - [1 – 8] с согласованием после 5 раунда
  - [9 – 16] с согласованием после 11 раунда
  - [17 – 24] с согласованием после 20 раунда
  - [25 – 32]
- Используется «Reflection property»:
  - Значение после 16 раундов известно и совпадет с шифртекстом
  - 4-ый интервал совпадает с 3-им
  - Значение после 24 итераций симметрично $\Rightarrow$ перебор 2^{32}
  - Значение после 8 итераций – перебор 2^{64}
- Материал 2^{32}
- Трудоемкость 2^{195}, память 2^{192}



Другие «результаты»

Серия работ:

- Алгебраический метод:
  - N. Courtois – «Security Evaluation of GOST 28147-89 In View Of International Standardisation»
  - N. Courtois – «Algebraic Complexity Reduction and Cryptanalysis of GOST»
  - N. Courtois – «Algebraic Complexity Reduction and Weak Keys in GOST»
  - ...
- Разностный метод:
  - N. Courtois, M. Misztal – «First Differential Attack On Full 32-Round GOST»
  - N. Courtois, M. Misztal – «Differential Cryptanalysis of GOST»
  - N. Courtois, M. Misztal – «An Improved Differential Attack on Full GOST»

Другие «результаты»

BEWARE

I'm going to cheat you
and totally ignore
the large data complexity
of many attacks…

$\Rightarrow$ just compare the running time

Courtois FSE 2012

Публикации по криптоанализу алгоритма ГОСТ 28147-89

1. Основные результаты
   - O. Kara – «Reflection Attacks on Product Ciphers» (INDOCRYPT 2008)
   - T. Isobe – «A Single-Key Attack on the Full GOST Block Cipher» (FSE 2011, JoC)
   - I. Dinur, O. Dunkelman, A. Shamir – «Improved Attacks on Full GOST» (ePrint, FSE 2012)
   - Bo Zhu, Guang Gong – «Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2»

2. Другие «результаты»
   - N. Courtois – «Algebraic Complexity Reduction and Cryptanalysis of GOST», и еще не менее 3 работ
   - N. Courtois, M. Misztal – «Differential Cryptanalysis of GOST», и еще не менее 2 работ

«Algebraic Complexity Reduction and Cryptanalysis of GOST»

Основная идея

- Использование структуры алгоритма шифрования
- Сведение задачи анализа E_K с большим количеством пар вход-выход к задаче анализа F_K с малым количеством пар вход-выход
- Представление F_K в виде системы нелинейных уравнений
- Решение полученной системы (XSL - метод)

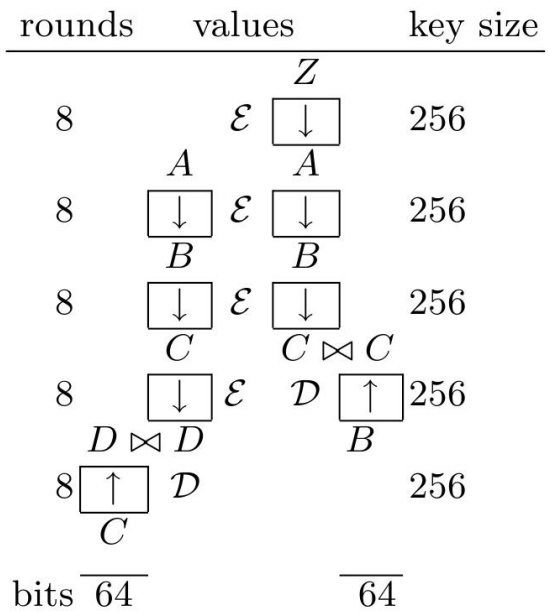
Реазультаты

- Снижение сложности алгебраического представления:
  - Предположения о специфических свойствах F_K
  - Перебор промежуточных значений
  - Получение пар вход-выход для F_K
  - порядка 20 различных подходов
- Получение и решение системы уравнений:
  - ??????

«Algebraic Complexity Reduction and Cryptanalysis of GOST»

Снижение сложности алгебраического представления

- Предположение: $A:\quad C = F_K^2(A)$ и $D = F_K^3(A)$ симметричны
- $E_K(A) = C$
- Из 2^{64} материала перебираются симметричные шифртексты (2^{32})
- Перебирается значение $B = F_K(A)$ (2^{64})
- $Z = E_K^{-1}(B)$
- 3 пары вход-выход для F_K: $A = F_K(Z)$, $B = F_K(A)$, $C = F_K(B)$,



Fact 3 (Key Recovery for 4 Rounds and 2 KP)

Given 2 P/C pairs for 4 rounds of GOST the 128-bit key can be recovered in time equivalent to 2^{24} GOST encryptions on the same software platform (it takes a few seconds). The memory requirements are very small. The attack works with a similar complexity for any choice of GOST S-boxes.

Fact 5 (Key Recovery for 8 Rounds and 3 KP)

Given 3 P/C pairs for 8 rounds of GOST we can produce 2^{64} candidates for the 256-bit key in time equivalent to 2^{120} GOST encryptions. The storage requirements are negligible and all the 2^{64} candidates can be produced in an uniform way, each of them is produced in time of 2^{56} GOST encryptions on average.
Remark: this result is particularly significant because it is close to 2^{128} which one could obtain in a Meet-In-the-Middle (MIM) attack and requires negligible storage

Публикации по криптоанализу алгоритма ГОСТ 28147-89

1. Основные результаты
   - O. Kara – «Reflection Attacks on Product Ciphers» (INDOCRYPT 2008)
   - T. Isobe – «A Single-Key Attack on the Full GOST Block Cipher» (FSE 2011, JoC)
   - I. Dinur, O. Dunkelman, A. Shamir – «Improved Attacks on Full GOST» (ePrint, FSE 2012)
   - Bo Zhu, Guang Gong – «Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2»

2. Другие «результаты»
   - N. Courtois – «Algebraic Complexity Reduction and Cryptanalysis of GOST», и еще не менее 3 работ
   - N. Courtois, M. Misztal – «Differential Cryptanalysis of GOST», и еще не менее 2 работ

«Differential Cryptanalysis of GOST»

Основная идея

- Использование «множественных» («aggregated») разностных соотношений: $\alpha \to \beta$, где $\alpha \in A$, $\beta \in B$
- Множественное разностное соотношение $(\Delta, \Delta) \to (\Delta, \Delta)$, где $\Delta = 0x80700700$
- Разностные характеристики:
  - 4R: $2^{-13.6}$ – эксперимент
  - 8R: $2^{-25} > (2^{-13.6})^2$ – эксперимент
  - 16R: $2^{-48} = (2^{-25})^2 \cdot 2^{2.2}$ – оценка (для случайного отображения 2^{-50})

Различные наборы подстановок

- Рассматривается тестовый набор узлов замены из ГОСТ Р 34.11-94
- We are not certain if it is possible at all to make a cipher such as GOST secure against differential cryptanalysis by changing only the S-boxes, which idea was discussed during the ISO standardization process of GOST
- Набор узлов из 1-го рабочего проекта дополнения к стандарту ISO/IEC 18033-3 «почему-то» не рассматривается

Выводы

Сравнительные характеристики различных атак

атака	модификация	сложность	память	материал
Isobe	reflection	2^{224}	2^{64}	2^{32}
Dinur et al.	fixed point - 2DMitM	2^{192}	2^{36}	2^{64}
	fixed point - low-memory	2^{204}	2^{19}	2^{64}
	reflection - 2DMitM	2^{224}	2^{36}	2^{32}
	reflection - low-memory	2^{236}	2^{19}	2^{32}
Zhu, Gong	reflection	2^{195}	2^{192}	2^{32}

Выводы

Слабости алгоритма ГОСТ 28147-89

- Ключевая развертка
  - Очевидное разложение в композицию двух преобразований (F_K и S)
  - Большое количество неподвижных точек у 16 последних раундов (Reflection)
  - Сведение к задаче криптоанализа F_K или F_K^2
  - Зависимость раундовых ключей от малого числа бит основного ключа
  - Возможность применения MitM-атак различного вида.
- Плохие рассеивающие свойства линейного преобразования
  - Возможность частичного вычисления промежуточных значений нескольких итераций – MitM-атака с малой памятью
  - Разностный метод

Выводы

- Результаты Isobe, Dinur et al. и Zhu, Gong показывают, что конструкция алгоритма ГОСТ 28147-89 не идеальна с теоретической точки зрения, однако не влияют на практическую стойкость алгоритма
- «Результаты» N. Courtios либо не обоснованы, либо не применимы при оптимальном выборе узлов замены
- Необходимо дополнение стандарта алгоритмом с длиной блока 128 бит