КОД безопасности

Отдел криптографического анализа

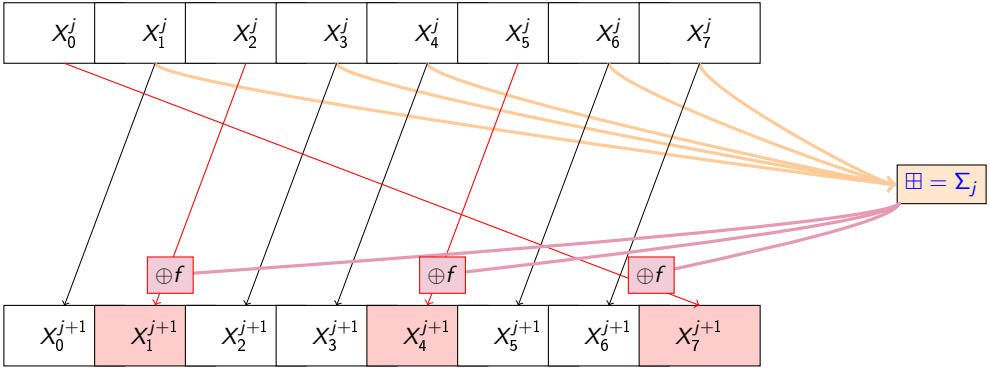
23 марта 2023 г.

Применение разностного метода к алгоритму КБ

Чухно А.Б.
Курочкин А.В.

КОД безопасности

Алгоритм КБ



КОД безопасности

Итерационное преобразование f

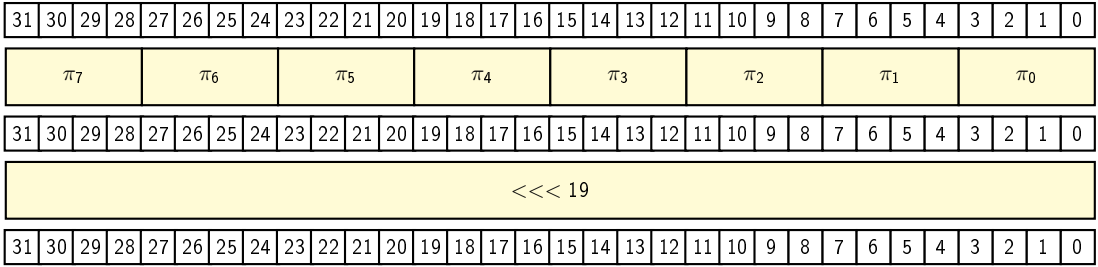


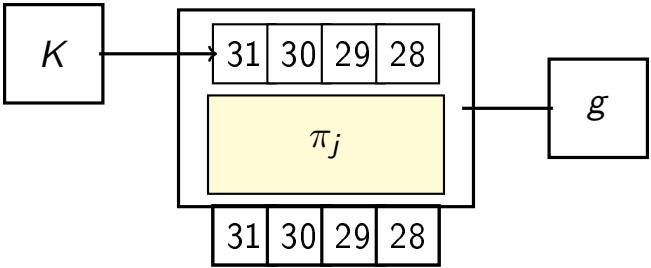
Рис.: Итерационное преобразование алгоритма КБ

Подстановки $\pi_0, \ldots, \pi_7$ – выбраны в соответствии с ГОСТ 34.12-2018 «Магма»

КОД безопасности

Нелинейные преобразования

Известно [1] [2], что модульное сложение может менять характеристики подстановок.



[1] Haruki Seki, Toshinobu Kaneko Differential Cryptanalysis of Reduced Rounds of GOST, Proceedings of the 7th Annual International Workshop on Selected Areas in Cryptography, 2001

[2] С. Яковлев, И. Гончар Проблема построения аналитических оценок стойкости к линейному криптоанализублочных шифров, использующих модульное сложение с ключом, XVI Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах», 2013

КОД безопасности

Нелинейные преобразования

$$\Sigma_j = X_1^j \boxplus X_2^j \boxplus X_4^j \boxplus X_6^j \boxplus X_7^j$$

КОД безопасности

Разностный путь

№ итерации	Входная разность	Выходная разность	вероятность выполнения соотношения
1	$(0, [31], 0, 0, 0, 0, [31], 0)$	$([31], 0, 0, 0, 0, [31], 0, 0)$	1
2	$([31], 0, 0, 0, 0, [31], 0, 0)$	$(0, 0, 0, 0, [31], 0, 0, [31])$	1
3	$(0, 0, 0, 0, [31], 0, 0, [31])$	$(0, 0, 0, [31], 0, 0, [31], 0)$	1
4	$(0, 0, 0, [31], 0, 0, [31], 0)$	$(0, 0, [31], 0, 0, [31], 0, 0)$	1
5	$(0, 0, [31], 0, 0, [31], 0, 0)$	$(0, [31], 0, 0, [31], 0, 0, 0)$	1
6	$(0, [31], 0, 0, [31], 0, 0, 0)$	$([31], 0, 0, [31], 0, 0, 0, 0)$	1
7	$([31], 0, 0, [31], 0, 0, 0, 0)$	$(0, [15], [31], 0, [15], 0, 0, [31, 15])$	2^{-9}
8	$(0, [15], [31], 0, [15], 0, 0, [31, 15])$	$([15], [15, 2, 1], 0, 0,$ $[15, 1, 0], 0, [31, 15], [31, 2, 0])$	$\approx 2^{-22.25}$
9	$([15], [15, 2, 1], 0, 0,$ $[15, 1, 0], 0, [31, 15], [31, 2, 0])$	$([15, 2, 1], 0, 0, [15, 1, 0],$ $0, [31, 15], [31, 2, 0], [15])$	$\approx 2^{-4}$
10	$([15, 2, 1], 0, 0, [15, 1, 0],$ $0, [31, 15], [31, 2, 0], [15])$	$(0, [19, 15, 2], [15, 1, 0], 0,$ $[31, 19, 2], [31, 15, 2, 0], [15], [31, 19])$	$\approx 2^{-35.25}$

КОД безопасности

Разностный путь

№ итерации	Входная разность	Выходная разность	вероятность выполнения соотношения
11	$(0, [19, 15, 2], [15, 1, 0], 0, [31, 19, 2],$ $[31, 15, 2, 0], [15], [31, 19])$	$([19, 15, 2], [15, 3, 1, 0], 0, [31, 19, 2],$ $[31, 15, 3, 2, 0], [15], [31, 19], [3])$	$\approx 2^{-19.25}$
12	$([19, 15, 2], [15, 3, 1, 0], 0, [31, 19, 2],$ $[31, 15, 3, 2, 0], [15], [31, 19], [3])$	$([15, 3, 1, 0], [19, 15], [31, 19, 2], [31, 15, 3, 2, 0],$ $[19], [31, 19], [3], [2])$	$\approx 2^{-33.43}$
13	$([15, 3, 1, 0], [19, 15], [31, 19, 2], [31, 15, 3, 2, 0],$ $[19], [31, 19], [3], [2])$	$([19, 15], [31, 20, 15, 2], [31, 15, 3, 2, 0], [19],$ $[31, 22, 20, 19, 15], [3], [2], [22, 3, 1])$	$\approx 2^{-33}$
14	$([19, 15], [31, 20, 15, 2], [31, 15, 3, 2, 0], [19],$ $[31, 22, 20, 19, 15], [3], [2], [22, 3, 1])$	$([31, 20, 15, 2], [31, 22, 15, 3, 2, 0],$ $[19], [31, 22, 20, 19, 15],$ $[22, 19, 3], [2], [22, 3, 1, 0], [20, 15])$	$\approx 2^{-33}$
15	$([31, 20, 15, 2], [31, 22, 15, 3, 2, 0],$ $[19], [31, 22, 20, 19, 15],$ $[22, 19, 3], [2], [22, 3, 1, 0], [20, 15])$	$([31, 22, 15, 3, 2, 0], [19, 2],$ $[31, 22, 20, 19, 15], [22, 19, 3],$ $0, [22, 3, 1, 0], [20, 15], [31, 20, 15])$	$\approx 2^{-35.2}$

Итоговая вероятность разностного соотношения равна $2^{-224.4}$

КОД безопасности

Эффективность разностного метода для полного алгоритма КБ

Надёжность	Сложность[3]
$0.99 \cdot 0.0527$	$2^{230} \cdot 2^{96}$
$0.5 \cdot 0.0527$	$2^{228} \cdot 2^{96}$
$10^{-2} \cdot 0.0527$	$2^{224} \cdot 2^{96}$
$10^{-3} \cdot 0.0527$	$2^{212} \cdot 2^{96}$

Построенное разностное соотношение хоть и имеет вероятность меньшую, чем 2^{256} , но всё еще не позволяет восстанавливать ключ эффективнее, чем полный перебор

[3] Число операций зашифрования

КОД безопасности

Эффективность разностного метода для алгоритма КБ, усечённого до 13 итераций

Надёжность	Сложность[4]
0.139	$2^{131} \cdot 2^{96}$
0.07	$2^{130} \cdot 2^{96}$
0.0014	$2^{126} \cdot 2^{96}$
0.00014	$2^{113} \cdot 2^{96}$

Для алгоритма КБ, усечённого до 13 итераций, разностное соотношение позволяет восстановить ключ эффективнее, чем полный перебор

[4] Число операций зашифрования