УДК 519.7

ОЦЕНКИ СЛОЖНОСТИ ДИФФЕРЕНЦИАЛЬНОЙ АТАКИ ПРИ РАЗЛИЧНЫХ ПАРАМЕТРАХ БЛОЧНОГО ШИФРА[1]

А. И. Пестунов

Дифференциальный криптоанализ [1] является распространенным подходом к построению атак на блочные шифры. Однако, как было замечено в [2], большинство существующих на сегодняшний день результатов криптоанализа блочных шифров представляют собой конкретные атаки на конкретные шифры. В работе [2] частично восполняется данный пробел. В предположении, что ключ является аддитивным, описывается дифференциальная атака в общем виде и сводится к решению системы уравнений.

В настоящей работе акцент делается на то, что в ряде случаев дифференциальная атака не является детерминированной, то есть она имеет вероятность успеха и неудачи. Под успехом понимается тот факт, что, отработав, атака на выходе даст верный искомый ключ. В частности, в работах, посвященных дифференциальному криптоанализу шифров MARS и CAST-256, описывались атаки, для которых подсчитывались вероятности успеха [3, 4].

Схемы этих атак похожи, различие заключается по сути только в дифференциальных характеристиках, на основании которых атаки строятся. В связи с этим возникает идея описать алгоритм в общем виде в зависимости от различных параметров блочного шифра и тем самым позволить криптоаналитику построить дифференциальную характеристику и автоматически получить вероятность успеха и сложность атаки, основанной на этой характеристике. Таким образом, криптоаналитик сфокусируется на специфических свойствах шифра, не отвлекаясь на построение атаки. В настоящей работе реализуется эта идея и рассчитывается сложность атаки при различных параметрах блочного шифра с целью достичь вероятности успеха не менее 99 %.

Дифференциальная атака в общем виде

Пусть имеется дифференциальная характеристика с разностью входных блоков Δ_{inp} и разностью выходных блоков Δ_{out}. Атака, направленная на отыскание подключа последнего раунда и основанная на данной характеристике, выглядит так:

1. Сформировать G групп различных пар блоков $A_t^g,\ B_t^g$ $(g = 1, ..., G;\ t = 1, ..., T)$ с разностью Δ_{inp}.
2. Для каждой из пар $(A_t^g,\ B_t^g)$ запросить пару шифртекстов $X_t^g = \text{Cipher}(A_t^g)$ и $Y_t^g = \text{Cipher}(B_t^g)$, полученные $G \cdot T$ пар шифртекстов сохранить в памяти.
3. Перебрать все возможные значения искомого подключа $k \in \{0, 1, ..., 2^n - 1\}$ и для каждого из них выполнить следующие действия:
   а) $g := 1$;
   б) с помощью последнего раунда и подключа k расшифровать сохраненные в памяти пары шифртекста из группы g и получить пары P_t^g и Q_t^g;
   в) если $P_t^g \oplus Q_t^g \neq \Delta_{\text{out}}$ для всех $t = 1, ..., T$, то k — это неправильный подключ-кандидат. Отбросить его и перейти к п. 3, где выбрать следующий подключ-кандидат; если хотя бы одна из пар обеспечивает условие $P_t^g \oplus Q_t^g = \Delta_{\text{out}}$, то перейти к п. *г*;

[1]Работа поддержана грантом в рамках Лаврентьевского конкурса молодежных проектов СО РАН 2010–2011 г.

г) если $g < G$, то $g := g + 1$ и перейти к п. *б*; иначе k — это верный подключ.

Параметры описанной атаки зависят от вероятности дифференциальной характеристики, параметров блочного шифра и желаемой вероятности успеха атаки. В данной работе параметры G и T подбирались таким образом, чтобы вероятность атаки составляла на менее 99 %. Затем полученные значения использовались для вычисления сложности атаки.

Результаты расчетов для некоторых параметров шифра приведены в таблице.

Расчет параметров атаки и ее сложности при различных параметрах шифра

Параметры шифра			Параметры атаки		Сложность		
Размер блока, бит	Размер перебираемого подключа, бит	Вероятность характеристики	Количество групп (G)	Количество пар блоков в группе (T)	Выбранные блоки	Память, байт	Количество шифрований
64	32	2^{-16}	1	2^{-19}	2^{20}	2^{23}	2^{53}
		2^{-32}	1	2^{-35}	2^{36}	2^{39}	2^{69}
		2^{-48}	2	2^{-51}	2^{53}	2^{56}	2^{86}
	64	2^{-16}	1	2^{-19}	2^{20}	2^{23}	2^{85}
		2^{-32}	2	2^{-35}	2^{37}	2^{40}	2^{102}
		2^{-48}	4	2^{-51}	2^{54}	2^{57}	2^{119}
	96	2^{-16}	2	2^{-19}	2^{21}	2^{24}	2^{118}
		2^{-32}	3	2^{-35}	2^{38}	2^{41}	2^{135}
		2^{-48}	6	2^{-51}	2^{55}	2^{58}	2^{152}
	128	2^{-16}	2	2^{-19}	2^{21}	2^{24}	2^{150}
		2^{-32}	4	2^{-35}	2^{38}	2^{41}	2^{167}
		2^{-48}	8	2^{-51}	2^{55}	2^{58}	2^{184}
128	32	2^{-16}	1	2^{-19}	2^{20}	2^{24}	2^{53}
		2^{-32}	1	2^{-35}	2^{36}	2^{40}	2^{69}
		2^{-48}	1	2^{-51}	2^{52}	2^{56}	2^{85}
		2^{-64}	1	2^{-67}	2^{68}	2^{72}	2^{101}
		2^{-80}	1	2^{-83}	2^{84}	2^{88}	2^{117}
		2^{-96}	1	2^{-99}	2^{100}	2^{104}	2^{133}
		2^{-112}	2	2^{-115}	2^{117}	2^{121}	2^{150}
	64	2^{-16}	1	2^{-19}	2^{20}	2^{24}	2^{85}
		2^{-32}	1	2^{-35}	2^{36}	2^{40}	2^{101}
		2^{-48}	1	2^{-51}	2^{52}	2^{56}	2^{117}
		2^{-64}	1	2^{-67}	2^{68}	2^{72}	2^{133}
		2^{-80}	1	2^{-83}	2^{84}	2^{88}	2^{149}
		2^{-96}	2	2^{-99}	2^{101}	2^{105}	2^{166}
		2^{-112}	4	2^{-115}	2^{118}	2^{122}	2^{183}
	96	2^{-16}	1	2^{-19}	2^{20}	2^{24}	2^{117}
		2^{-32}	1	2^{-35}	2^{36}	2^{40}	2^{133}
		2^{-48}	1	2^{-51}	2^{52}	2^{56}	2^{149}
		2^{-64}	1	2^{-67}	2^{68}	2^{72}	2^{165}
		2^{-80}	2	2^{-83}	2^{85}	2^{89}	2^{182}
		2^{-96}	3	2^{-99}	2^{102}	2^{106}	2^{199}
		2^{-112}	6	2^{-115}	2^{119}	2^{123}	2^{216}
	128	2^{-16}	1	2^{-19}	2^{20}	2^{24}	2^{149}
		2^{-32}	1	2^{-35}	2^{36}	2^{40}	2^{165}
		2^{-48}	1	2^{-51}	2^{52}	2^{56}	2^{181}
		2^{-64}	2	2^{-67}	2^{69}	2^{73}	2^{198}
		2^{-80}	2	2^{-83}	2^{85}	2^{89}	2^{214}
		2^{-96}	4	2^{-99}	2^{102}	2^{106}	2^{231}
		2^{-112}	8	2^{-115}	2^{119}	2^{123}	2^{248}

ЛИТЕРАТУРА

1. *Biham E., Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptol. 1991. V. 4. P. 3–72.
2. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1(1). С. 34–42.
3. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра MARS // Прикладная дискретная математика. 2009. № 4(6). С. 56–63.
4. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информационных технологий. 2009. № 4. С. 57–62.

УДК 519.7

О СЛАБОМ КЛАССЕ АЛГОРИТМОВ РАЗВЁРТЫВАНИЯ КЛЮЧА ОТНОСИТЕЛЬНО МЕТОДА СВЯЗАННЫХ КЛЮЧЕЙ[1]

М. А. Пудовкина

В открытой литературе появляется всё больше работ, посвященных атакам на алгоритмы шифрования на основе метода связанных ключей и основанных на слабостях алгоритма развёртывания ключа (см., например, [1 – 8]). Однако имеется небольшое число работ, в которых описываются классы слабых алгоритмов развёртывания ключа или исследуются их свойства. Данную работу можно отнести к их числу.

Обозначим: $\mathbb{N}$ — множество натуральных чисел; $\mathbb{N}_0$ — множество натуральных чисел с нулем; $n, r, d, l \in \mathbb{N}$; V_n — n-мерное векторное пространство над полем $\mathrm{GF}(2)$; l — число раундов шифрования блочного алгоритма; $2 \leqslant r < l$; $g_k : V_n \to V_n$ — раундовая функция; $K = V_d$ — ключевое множество.

В данной работе рассматриваются функция зашифрования и алгоритм развёртывания ключа $\varphi^* = (\delta, \varphi)$, такие, что существуют число $r \in \mathbb{N}$, $r \leqslant l$, и отображения $\lambda : V_n^r \to V_n$, $\delta : K \to V_n^r$, $\varphi : V_n^r \to V_n^l$, удовлетворяющие следующим свойствам:

1) $(r-1) \cdot n < d \leqslant r \cdot n$;
2) $\delta(k) = (k_0, ..., k_{r-1})$;
3) для любого $i \in \mathbb{N}_0$ выполняется равенство

$$(k_i, ..., k_{i+l-1}) = \varphi(k_i, ..., k_{i+r-1}),$$

где $k_{i+l+j} = \lambda(k_{i+j}, ..., k_{i+r-1+j})$, $j = 0, ..., l-r$;
4) раундовая функция на всех раундах не зависит от номера раунда;
5) $g_k \neq g_{k'}$ для любых различных $k, k' \in V_n$;
6) существует такая функция $\psi : V_n \times V_n \to V_n$, что для всех $k \in V_n$, $\alpha \in V_n$ выполняется равенство $k = \psi(\alpha, \beta)$, где $\beta = \alpha^{g_k}$.

Отметим, что условие 5 является естественным и встречается практически во всех алгоритмах блочного шифрования в открытой литературе. Условие 2 означает, что по любой последовательности из r раундовых ключей $k_i, ..., k_{i+r-1}$ для некоторого $i \in \{0, ..., l-r\}$ может быть найден ключ шифрования $k \in K$. Чаще всего ключ шифрования k совпадает с вектором $(k_0, ..., k_{r-1})$, т. е. δ — тождественное отображение. Отметим также, что условие 6 может иногда не выполняться. Кроме того, отображение φ

[1]Работа выполнена при поддержке гранта Президента РФ НШ № 4.2008.10.