ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 26 МАТЕМАТИКИ Выпуск 3
2019

В. А. Кирюхин, (Москва, ОАО «ИнфоТеКС»). **Атака методом бумеранга на связанных ключах на 5 раундов шифра Кузнечик.**

Атака методом бумеранга на блочный шифр была предложена в [2]. В работе [3] метод бумеранга был применен для атаки с использованием связанных ключей.

В работе [4] была предложена атака на связанных ключах на 5-раундовый шифр Кузнечик [1], формула шифрпреобразования которого имеет вид

$$\begin{aligned}\mathsf{E}_K(A) = \mathsf{E}_{K_1,K_2}(A) = \mathsf{X}[K_6]\mathsf{LSX}[K_5]\mathsf{LSX}[K_4]\mathsf{LSX}[K_3]\mathsf{LSX}[K_2]\mathsf{LSX}[K_1](A),\\ K_3 = K_1 \oplus \mathsf{LSX}[C_2](K_2 \oplus \mathsf{LSX}[C_1](K_1)),\\ K_4 = K_2 \oplus \mathsf{LSX}[C_1](K_1),\\ K_5 = K_3 \oplus \mathsf{LSX}[C_4](K_4 \oplus \mathsf{LSX}[C_3](K_3)),\\ K_6 = K_4 \oplus \mathsf{LSX}[C_3](K_3).\end{aligned}$$

Трудоемкость упомянутой атаки 2^{32} операций, 2^{16} связанных ключей, 2^{30} памяти.

В рамках модели связанных ключей атакующий имеет возможность зашифровать и дешифровать любой текст с использованием ключей $K = K_1||K_2$ и $\widetilde{K} = \widetilde{K}_1||\widetilde{K}_2$. Ключи K и $\widetilde{K}$ неизвестны атакующему, но известна связь между ними $K \oplus \widetilde{K} = \Delta K_1||\Delta K_2$.

Выберем $\Delta K_1 = 0$, $\Delta K_2 = \kappa$, где κ содержит один ненулевой байт, тогда $\Delta K_4 = \kappa$, а число возможных ΔK_3 не превосходит 2^7.

Возьмем произвольный открытый текст P и получим два соответствующих шифртекста $Q = \mathsf{E}_K(P)$ и $\widetilde{Q} = \mathsf{E}_{\widetilde{K}}(P)$. Выберем разность δ так, чтобы в $\mathsf{L}^{-1}(\delta)$ был один ненулевой байт. Возьмем шифртексты $Z = Q \oplus \delta$, $\widetilde{Z} = \widetilde{Q} \oplus \delta$ и соответствующие открытые тексты $W = \mathsf{E}_K^{-1}(Z)$, $\widetilde{W} = \mathsf{E}_{\widetilde{K}}^{-1}(\widetilde{Z})$.

Известна разность $\Delta W = W \oplus \widetilde{W}$. Обозначим $Y = \mathsf{LSX}[K_1](W)$, $\widetilde{Y} = \mathsf{LSX}[K_1](\widetilde{W})$. Тогда вероятность того, что $\Delta Y = Y \oplus \widetilde{Y}$ имеет только один ненулевой байт, можно оценить снизу значением $p = 2^{-21}$:

$$\begin{gathered}\Pr\left(\mathsf{LSX}[K_2]\mathsf{LSX}[K_1](P) \oplus \mathsf{LSX}[\widetilde{K}_2]\mathsf{LSX}[K_1](P) = \Delta K_3\right) \geqslant 2^{-7},\\ \Pr\left(\nabla = \widetilde{\nabla}\right) \geqslant 2^{-7},\\ \Pr\left(\mathsf{S}^{-1}(\mathsf{S}(D) \oplus \nabla) \oplus \mathsf{S}^{-1}(\mathsf{S}(D \oplus \kappa) \oplus \nabla) = \kappa\right) \geqslant 2^{-7},\\ \text{где } \nabla = \mathsf{L}^{-1}\mathsf{X}[K_5]\mathsf{S}^{-1}\mathsf{L}^{-1}\mathsf{X}[K_6](Z) \oplus \mathsf{L}^{-1}\mathsf{X}[K_5]\mathsf{S}^{-1}\mathsf{L}^{-1}\mathsf{X}[K_6](Q),\\ \widetilde{\nabla} = \mathsf{L}^{-1}\mathsf{X}[\widetilde{K}_5]\mathsf{S}^{-1}\mathsf{L}^{-1}\mathsf{X}[\widetilde{K}_6](\widetilde{Z}) \oplus \mathsf{L}^{-1}\mathsf{X}[\widetilde{K}_5]\mathsf{S}^{-1}\mathsf{L}^{-1}\mathsf{X}[\widetilde{K}_6](\widetilde{Q}),\\ D = \mathsf{X}[K_4]\mathsf{LSX}[K_3]\mathsf{LSX}[K_2]\mathsf{LSX}[K_1](P).\end{gathered}$$

Для каждой пары W, $\widetilde{W}$ опробуется 255 вариантов ΔY и строится множество возможных ключей K_1, удовлетворяющих соотношению

$$\mathsf{S}(K_1 \oplus W) \oplus \mathsf{S}(K_1 \oplus \widetilde{W}) = \mathsf{L}^{-1}(\Delta Y).$$

Известно [6], что в среднем каждый набор W, $\widetilde{W}$, ΔY будет давать один вариант ключа K_1. Для определения истинного ключа K_1 потребуется в среднем $2 \cdot p^{-1}$ текстов W, $\widetilde{W}$, при этом истинный ключ встретится дважды, любой ложный ключ — только один раз.

Трудоемкость предложенной атаки $2^{34} = p^{-1} \cdot 2 \cdot 255 \cdot 16$ операций доступа к памяти, два связанных ключа, $2^{24} = p^{-1} \cdot 2 \cdot 4$ адаптивно выбираемых пар ОТ/ШТ, $2^{29} = p^{-1} \cdot 2 \cdot 255 \cdot 2^{-1}$ 16-байтовых блоков памяти.

Экспериментальная проверка показала корректность оценок трудоемкости атаки. Оценка вероятности p может быть увеличена за счет выбора конкретных κ и δ с использованием подходов, изложенных в [5].

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 34.12-2015. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
2. *David Wagner.* The Boomerang Attack — FSE '99, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1999, v. 1636, p. 156–170.
3. *Eli Biham*, *Orr Dunkelman*, *Nathan Keller.* Related-Key Boomerang and Rectangle Attacks — Advances in Cryptology, EUROCRYPT 2005, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2005, v. 3494, p. 507–525.
4. *Kiryukhin V.* Related-key Attack on 5-round Kuznyechik. 8th Workshop on Current Trends in Cryptology (CTCrypt 2019), 2019.
5. *Carlos Cid*, *Tao Huang*, *Thomas Peyrin*, *Yu Sasaki*, *Ling Song.* Boomerang Connectivity Table: A New Cryptanalysis Tool. Advances in Cryptology, EUROCRYPT 2018, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2018, v. 10821, p. 683–714.
6. *Patrick Derbez*, *Pierre-Alain Fouque*, *Jérémy Jean.* Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting. Advances in Cryptology, EUROCRYPT 2013, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2013, v. 7881, p. 371–387.