Частичное маскирование шифра «Кузнечик»

Щербакова Анна Олеговна,
Жиляев Андрей Евгеньевич.
«ИнфоТеКС»

Маскирование

- ***Принцип:*** разделение каждого значимого промежуточного значения на d долей

$$x = x_1 \oplus x_2 \oplus \cdots \oplus x_d$$

- ***Проблема:*** производительность снижается в $O(d^2)$ раз.
- ***Решение***: частичное маскирование
- ***Вопрос:*** какое количество раундов необходимо маскировать?

Модель злоумышленника

- в рамках раунда шифра нельзя получить более d значений функции утечки $L_i = L(x_i)$;
- известны используемые открытые тексты и шифртексты;
- нет доступа к ключевому расписанию;
- можно исполнять алгоритм неограниченное число раз, менять выбор мест, с которых снимаются значения;
- раундовые ключи подаются в уже маскированном виде в тех раундах, где необходимо маскирование.

Метод анализа

Предлагается метод:

«*Ориентированный на безопасность анализ потоков данных*»

(Security-oriented Data Flow Analysis, SDFA)

Prouff M., Rivain E. «Provably Secure Higher-Order Masking of AES», CHES, LNCS, vol. 6225, 2010.

Метод анализа

- **Общая идея анализа:** при маскировании влияние бит ключа на биты внутренних переменных становится наибольшим на средних раундах, а к крайним раундам влияние бит ключа ослабевает. Можно избежать маскирования на средних раундах, оставив только на крайних.

- **Результат анализа:** Раунд Кузнечика замешивает раундовый ключ так, что каждый бит выходного значения раунда зависит от всех бит раундового ключа. Соответственно, необходимо маскировать по 2 раунда с начала и с конца

Результаты

Реализация: L и X аддитивно, S таблично.
Количество масок: $2d + 1$ маска для всех преобразований.
Теоретические оценки замедления:

- Преобразование X – в $O(2d + 1)$ раз.
- Преобразование L – в $O(2d + 1)$ раз.
- Преобразование S – в $O((2d + 1)^2)$ раз.

Случайная информация: $4096(d - 1)^2 + 128(d - 1)$ байт для 1 блока данных
Скорость генератора: ~200Гб/сек для шифрования со скоростью 100 Мб/с при $d = 3$
Вывод: нужно искать преставление S в «удобном» аналитическом виде

Результаты: возможные варианты

- ***Предположение:*** съем побочной информации с S сложнее, чем с L и X
- ***Идея***: маскирование только линейных операций
- ***Результат***: скорость генератора случайных чисел ~2 Гигабайта/сек;

Заключение

Маскирование всего блочного шифра – высоко затратная операция с существенной потерей производительности.

Предложенный алгоритм определения количества раундов для маскирования позволяет существенно снизить необходимые затраты ресурсов при ограничениях, используемых в модели.

infotecs

Вопросы?

Щербакова Анна Олеговна,
Жиляев Андрей Евгеньевич.
«ИнфоТеКС»