Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7 DOI 10.17223/2226308X/14/12

XS-СХЕМЫ: СКРЫТИЕ ТАКТОВЫХ ОРАКУЛОВ

С. В. Агиевич

XS-схемы описывают блочные шифры, в которых используются две операции над двоичным словами фиксированной длины: X — поразрядное сложение по модулю 2 и S — подстановка. В работе исследуется модель XS-схем, согласно которой несколько экземпляров простой тактовой схемы, в которой задействована всего одна операция S, объединяются в сложную схему, называемую каскадом. S-операции каскадов интерпретируются как независимые тактовые оракулы. Возможность определения пары «вход — выход» некоторого оракула по паре «вход — выход» всего каскада означает слабость последнего. Мы формализуем свойство каскада скрывать тактовых оракулов, т. е. затруднять определение внутренних пар «вход — выход». Мы показываем, что при использовании регулярной тактовой схемы каскад скрывает оракулов, если число тактов не менее чем в 2 раза больше размерности (числа слов в обрабатываемом блоке данных).

Ключевые слова: *блочный шифр, XS-схема, тактовый оракул, линейная рекуррентная последовательность.*

В [1] для описания блочно-итерационных шифров предложено использовать XS-схемы. Элементарная (однотактовая) XS-схема порядка n задаётся тройкой (a, B, c), в которой a и c — двоичные вектор-столбец и вектор-строка размерности n, B — двоичная матрица порядка n. Схема инстанциируется над полем $\mathbb{F}$ из 2^m элементов выбором подстановки $S\colon \mathbb{F} \to \mathbb{F}$, которая называется *тактовым оракулом*. Результатом инстанциирования является преобразование

$$(a, B, c)[S]\colon \mathbb{F}^n \to \mathbb{F}^n,\ x \mapsto y = xB + S(xa)c.$$

Здесь и далее x и y — вектор-строки.

Нас будут интересовать регулярные схемы, только они имеют криптографическое значение. В регулярной схеме матрицы

$$A = \begin{pmatrix} a & Ba & \dots & B^{n-1}a \end{pmatrix}, \quad C = \begin{pmatrix} cB^{n-1} \\ \dots \\ cB \\ c \end{pmatrix}$$

обратимы. Матрица B может быть обратимой или нет, в зависимости от этого схему относят к типу I или II.

Пусть $(a, B, c)^t$ — t-тактовый каскад, полученный соединением t экземпляров элементарной схемы (a, B, c). Инстанциируя экземпляры оракулами $S_1, \dots, S_t$, получаем преобразование $(a, B, c)^t[S_1, \dots, S_t]$. Его действие можно описать следующим образом: по входу $x = y(0) \in \mathbb{F}^n$ вычисляется последовательность

$$y(\tau) = y(\tau - 1)B + S_\tau(y(\tau - 1)a)c, \quad \tau = 1, 2, \dots, t,$$

и её последний элемент $y = y(t)$ объявляется результатом преобразования.

Оракулы S_τ моделируют секретные подстановки, действие которых определяется тактовыми ключами, построенными по исходному ключу блочного шифра. Как правило, тактовый ключ достаточно легко определить всего по одной паре «вход — выход» соответствующего оракула. Поэтому важно, чтобы каскад скрывал своих оракулов в смысле следующего определения.

Определение 1. Каскад $(a, B, c)^t$ размерности n над полем $\mathbb{F}$ из 2^m элементов *скрывает тактовых оракулов*, если в описываемой ниже игре симулятора с противником последний не может добиться успеха с вероятностью отличной от $1/2^m$. Правила игры:

1) Симулятор выбирает случайные независимые равновероятные подстановки S_1, $S_2, \ldots, S_t$ над $\mathbb{F}$. Они будут использоваться в качестве тактовых оракулов.
2) Противник выбирает вектор $x \in \mathbb{F}^n$ и передает его симулятору.
3) Симулятор вычисляет вектор $y = (a, B, c)^t[S_1, S_2, \ldots, S_t](x)$ и возвращает его противнику.
4) Получив y, противник выбирает номер такта $\tau \in \{1, 2, \ldots, t\}$, определяет пару $(\hat{u}, \hat{v}) \in \mathbb{F} \times \mathbb{F}$ и передает её симулятору.
5) Симулятор подводит итог: противник победил, если $\hat{v} = S_\tau(\hat{u})$, и проиграл, если равенство нарушается.

В ходе игры противник демонстрирует умение определять «входы — выходы» тактовых оракулов, а симулятор проверяет это умение. Под противником понимается вероятностный алгоритм. Обратим внимание, что ограничения на его вычислительные ресурсы (время, память) не накладываются. Порог вероятности $1/2^m$ означает, что противник может лишь угадать выход $S_\tau(\hat{u})$ на входе $\hat{u}$ (или вход $S_\tau^{-1}(\hat{v})$ на выходе $\hat{v}$), т. е. каскад действительно скрывает оракулов.

Пусть $u_\tau \in \mathbb{F}$ — вход оракула S_τ во время обработки x и $v_\tau = S_\tau(u_\tau)$ — соответствующий выход, $\tau = 1, 2, \ldots, t$. Векторы x и y связаны следующим образом:

$$y = xB^t + (v_1, v_2, \ldots, v_t)C_t.$$

Здесь C_t — матрица размера $t \times n$, в которой τ-я строка — это вектор $cB^{t-\tau}$.

В силу регулярности матрица C_t обратима при $t = n$. Поэтому по паре (x, y) можно определить вектор $(v_1, v_2, \ldots, v_t)$ выходов тактовых оракулов, а затем и входы:

$$u_\tau = xB^{\tau-1}a + \sum_{i=1}^{\tau-1} v_i cB^{\tau-1-i}a, \quad \tau = 1, 2, \ldots, t.$$

Таким образом, n-тактовый каскад не скрывает оракулов, и число тактов необходимо увеличивать. Следующая теорема показывает, что для скрытия достаточно $2n$ тактов.

Теорема 1. Если (a, B, c) — регулярная схема и $t \geqslant 2n$, то каскад $(a, B, c)^t$ скрывает тактовых оракулов.

Доказательство. Начнём с рассмотрения схем типа I. Предположим, что существует обратимая матрица M размера $n \times n$ над полем $\mathbb{F}$, такая, что $C_t M$ содержит столбец с единственным ненулевым элементом. Пусть, не нарушая общности, это столбец e_τ с единицей в позиции τ и нулями в остальных позициях. Если e_τ — это i-й столбец $C_t M$, то v_τ можно найти как i-ю координату $(xB^t + y)M$, поскольку

$$(v_1, v_2, \ldots, v_t)C_t M = (xB^t + y)M.$$

При запрете на существование M матрица C_t, дополненная столбцом e_τ, имеет полный ранг $n+1$. Данный факт выполняется для любого номера $\tau = 1, 2, \ldots, t$. Факт означает, что при любом варианте выбора выхода v_τ имеется одно и то же число вариантов выбора остальных выходов, при которых x переходит в y. Поскольку случайный равновероятный выбор $S_1, S_2, \ldots, S_t$ индуцирует случайный равновероятный выбор вектора выходов $(v_1, v_2, \ldots, v_t)$ при любом векторе входов $(u_1, u_2, \ldots, u_t)$, все варианты перехода $x \mapsto y$ имеют один и тот же вероятностный вес. Поэтому вероятность корректно определить v_τ равняется $1/2^m$. С такой же вероятностью окажется корректной любая пара $(\hat{u}, \hat{v})$, выбранная противником.

Остаётся показать, что матрицы M не существует. Предположим противное. Пусть r — некоторый (ненулевой) столбец M. Записывая координаты соответствующего столбца $C_t M$ снизу вверх, получаем последовательность

$$cB^0 r, cB^1 r, \ldots, cB^{t-1} r.$$

Мы имеем дело с линейной рекуррентной последовательностью (л.р.п.) порядка n. Л.р.п. ненулевая, поскольку её n-префикс ненулевой. Префикс действительно ненулевой, поскольку матрица C из определения регулярности обратима. Более того, из обратимости C следует, что любой n-отрезок л.р.п. будет ненулевым. Поэтому отрезок длины $t \geqslant 2n$ не может содержать менее двух ненулевых элементов. Другими словами, столбец $C_t M$ не может содержать только один ненулевой элемент. Противоречие.

Рассмотрим теперь регулярные схемы типа II. Для них л.р.п. $(cB^\tau r)$ снова начинается с ненулевого n-префикса. Поскольку B вырождена, после префикса могут идти одни нули. Поэтому можно точно определить выход S_τ для $\tau \in \{t-n+1, t-n+2, \ldots, t\}$. Выходы для остальных τ можно определить только с вероятностью $1/2^m$. Аналогичные рассуждения применимы к обратному преобразованию F^{-1}. Оно имеет тот же тип II, и в нём в обратном порядке задействованы обратные оракулы S_τ^{-1}. Теперь можно определить выход S_τ^{-1}, т. е. вход S_τ, для $\tau \in \{1, 2, \ldots, n\}$. Другие входы определяются с вероятностью $1/2^m$. Итак, вероятность успешного определения пары (u_τ, v_τ) целиком не превосходит $1/2^m$. Поэтому любая пара $(\hat{u}, \hat{v})$, выбранная противником, окажется корректной с вероятностью $1/2^m$. ■

Открытым остаётся вопрос о скрытии тактовых оракулов, когда противник может выбрать не один, а несколько входов x и получить соответствующие выходы $y = (a, B, c)^t[S_1, S_2, \ldots, S_t](x)$.

ЛИТЕРАТУРА

1. *Agievich S.* XS-circuits in block ciphers // Матем. вопр. криптогр. 2019. Т. 10. № 2. С. 7–30.