УДК 001.817

О 2-ТРАНЗИТИВНОСТИ XS-СХЕМ

С. В. Агиевич

НИИ прикладных проблем математики и информатики,
Белорусский государственный университет,
Минск, Беларусь, agievich@bsu.by

XS-схемы описывают тактовые тактовые подстановки широкого класса блочных шифров. Для защиты от атаки по невозможным дифференциалам лежащая в основе шифра схема должна быть 2-транзитивной, а число тактов не меньше индекса 2-транзитивности. В работе вводится необходимое и почти достаточное условие 2-транзитивности XS-схемы, улучшается оценка сверху для индекса 2-транзитивности.

Ключевые слова: блочный шифр; тактовая подстановка; *S*-блок; схема; 2-транзитивность.

ON 2-TRANSITIVITY OF XS-CIRCUITS

S. V. Agievich

Research Institute for Applied Problems of Mathematics and Informatics,
Belarusian State University,
Minsk, Belarus, agievich@bsu.by

XS-circuits describe round permutations of a wide class of block ciphers. To protect a cipher against an impossible differential attack, the underlying circuit must be 2-transitive and the number of rounds must be at least the index of 2-transitivity. We provide a necessary and almost sufficient condition for 2-transitivity of an XS-circuit. We also improve the upper bound on the index of 2-transitivity.

Keywords: block cipher; round permutation; *S*-box; circuit; 2-transitivity.

1. Введение

XS-схемы, введенные в работе [1], описывают тактовые преобразования широкого класса блочных шифров. Схема размерности n задается тройкой (a, B, c), в которой a — вектор-столбец размерности n, B — квадратная матрица порядка n, c — вектор-строка размерности n. Координаты векторов и элементы матрицы лежат в поле $\mathbb{F}_2$. Схема (a, B, c) уточняется дополнительными параметрами: полем $\mathbb{F}$ — некоторым расширением $\mathbb{F}_2$

и S-блоком S — подстановкой на $\mathbb{F}$. Уточненная схема задает следующее преобразование вектор-строк $x \in \mathbb{F}^n$:

$$(a, B, c)[S](x) = xB + S(xa)c.$$

Будем рассматривать обратимые схемы — те, для которых данное преобразование обратимо при любом выборе $\mathbb{F}$ и S. Условия обратимости даны в работе [1]. Обратные преобразования обратимой схемы (a, B, c) также описываются XS-схемой. Будем обозначать ее $(a, B, c)^{-1}$. В блочном шифре преобразования схемы (a, B, c) с разными (вообще говоря) ключезависимыми S-блоками объединяются в композиционные каскады, называясь при этом тактовыми преобразованиями или просто тактами. На вход каскада в качестве x подается открытый текст, с выхода снимается шифртекст. Преобразования t-тактового каскада с S-блоками $S_1, S_2, \ldots, S_t$ обозначаются через $(a, B, c)^t[S_1, S_2, \ldots, S_t]$.

Для обеспечения базовых гарантий криптографической стойкости схема (a, B, c) должна быть регулярной: во-первых, обратимой и, во-вторых, давать обратимые матрицы $A = \left(a \; Ba \ldots B^{n-1}a\right)$ и $C = \left((cB^{n-1})^T \ldots (cB)^T \; c^T\right)^T$.

Расширенные гарантии связаны с защитой от тех или иных криптоаналитических атак. Так для защиты от атаки по невозможным дифференциалам (Impossible Differential Attack, IDA, см. [3]) схема должна быть 2-транзитивной, причем индекс 2-транзитивности должен быть по возможности невелик (определения будут даны позже).

Исследование 2-транзитивности было начато нами в работе [1]: было найдено необходимое условие 2-транзитивности (*сильная регулярность*) и получены оценки сверху для индекса 2-транзитивности при выполнении данного условия.

В настоящей работе мы усиливаем результаты [1]. Во-первых, предлагаем более слабое необходимое условие 2-транзитивности: *плотность профиля* схемы. Во-вторых, показываем, что для регулярной схемы при необременительных ограничениях на ее размерности плотность профиля является также достаточным условием 2-транзитивности. В-третьих, усиливаем оценки сверху для индекса 2-транзитивности, задействуя новую характеристику схем: *порог полного ранга*.

Будем использовать канонические формы регулярных схем (a, B, c). У первой формы $c = (0, \ldots, 0, 1)$, у второй $a = (1, 0, \ldots, 0)^T$. У обеих форм одна и та же матрица B, она представляет собой клетку Фробениуса.

Для натурального M через $M^{[n]}$ будем обозначать n-ую факториальную степень $M : M^{[n]} = M(M-1)\ldots(M-n+1)$.

2. Результаты

Определение 1. *Профиль* схемы (a, B, c) — это двоичная последовательность $\sigma = (\sigma_t)$, в которой

$$\sigma_t = cB^{t-1}a,\ t = 1, 2, \ldots.$$

Профиль является линейной рекуррентной последовательностью (л.р.п.), порядок которой совпадает с размерностью (a, B, c), а характеристический многочлен — с характеристическим многочленом B. Пусть схема имеет размерность n, B — клетка Фробениуса и $b = (b_1, b_2, \ldots, b_n)^T$ — последний столбец B. Тогда

$$\sigma_t = \sum_{i=1}^{n} b_{n+1-i}\sigma_{t-i},\ t = n+1, n+2, \ldots$$

при начальных условиях $(\sigma_1, \ldots, \sigma_n) = (ca, cBa, \ldots, cB^{n-1}a) = cA.$

Начальные условия не могут быть нулевыми, если (a, B, c) — регулярная схема, т. е. A и C обратимы. Действительно, в силу обратимости A противное означает, что $c = 0$. Но тогда $C = 0$, противоречие.

Особенно просто начальные условия выглядят, когда (a, B, c) записана во второй канонической форме, т.е. $a = (1, 0, \ldots, 0)^T$. В этом случае A — единичная матрица и $cA = c$.

Важно, что профиль не меняется при переходе от (a, B, c) к подобной схеме $(P^{-1}a, P^{-1}BP, cP)$, где P — обратимая матрица порядка n.

Более того, регулярная схема (a, B, c) размерности n восстанавливается с точностью до подобия по начальному $2n$-отрезку своего профиля σ.

Определение 2. Для последовательности $\sigma = (\sigma_t)$ обозначим $\mathrm{supp}(\sigma) = \{r \in \mathbb{N} : \sigma_r \neq 0\}$ и пусть $\langle \mathrm{supp}(\sigma) \rangle$ — множество, составленное из всевозможных сумм элементов supp(σ). Последовательность σ называется *плотной* (dense), если найдется неотрицательное целое t_0 такое, что всякое $t \geq t_0$ лежит в $\langle \mathrm{supp}(\sigma) \rangle$.

Лемма. *Последовательность* σ *плотна тогда и только тогда, когда найдутся* $r_1, r_2, \ldots, r_k \in \mathrm{supp}(\sigma)$ *такие, что* $\gcd(r_1, r_2, \ldots, r_k) = 1$.

Доказательство. Если подходящий набор $(r_1, r_2, \ldots, r_k)$ существует, то найдется конечное $t_0 = t_0(r_1, r_2, \ldots, r_k)$ такое, что любое $t \geq t_0$ можно представить в виде суммы элементов набора. Данный факт доказан в рамках решения задачи Фробениуса (см. напр. [2]). Факт означает, что σ является плотной.

Наоборот, если подходящий набор не существует, то ненулевые элементы σ либо расположены в позициях, кратных некоторому $d > 1$, либо вообще отсутствуют. В обоих случаях σ не является плотной. Действительно, в первом случае представление t в виде суммы нельзя реализовать для t не кратных d, а во втором — ни для одного t. □

Лемма означает, что если ненулевая последовательность σ не является плотной, то она разрежена с шагом $d > 1$: ненулевые элементы отстоят друг от друга на величины, кратные d. Термин «плотная» выбран нами как альтернатива «разреженная».

Тот факт, что профиль представляет собой линейную рекуррентную последовательность, упрощает проверку плотности.

Теорема 1. *Пусть* (a, B, c) *— регулярная схема размерности* n, *в которой* B *— клетка Фробениуса, и* $(b_1, b_2, \ldots, b_n)^T$ *— ее последний столбец. Пусть* $r_1, r_2, \ldots, r_k$ *— номера единиц в векторах* cA *и* $(b_n, b_{n-1}, \ldots, b_1)$ *при нумерации координат слева направо от* 1. *Профиль* σ *схемы* (a, B, c) *плотен тогда и только тогда, когда* $\gcd(r_1, r_2, \ldots, r_k) = 1$.

Если $c = (0, \ldots, 0, 1)$, т.е. (a, B, c) записана в первой канонической форме, и $a = (a_1, a_2, \ldots, a_n)^T$, то вектор cA может быть заменен на $(a_n, a_{n-1}, \ldots, a_1)$.

Теорема 2. *Профиль регулярной схемы* (a, B, c) *плотен тогда и только тогда, когда плотен профиль обратной схемы* $(a, B, c)^{-1}$.

Для натуральных t и $\tau_1, \tau_2, \ldots, \tau_k \leq t$ введем в рассмотрение матрицу

$$C(t; \tau_1, \tau_2, \ldots, \tau_k) = \begin{pmatrix} cB^{t-\tau_1} \\ cB^{t-\tau_2} \\ \ldots \\ cB^{t-\tau_k} \end{pmatrix}.$$

Определение 3. Пусть (a, B, c) — регулярная схема размерности n, σ — ее профиль. *Порог полного ранга* схемы — это минимальное t, для которого найдутся натуральные $t_1, t_2, \ldots, t_n \leq t$ такие, что $t_i \in \langle \operatorname{supp}(\sigma) \rangle$ и матрица $C(t; t_1, t_2, \ldots, t_n)$ обратима.

Порог обозначается через frt(a, B, c), от англ. “full-rank threshold”. Порог полагается равным ∞, если подходящий набор $t_1, t_2, \ldots, t_n$ не существует ни для одного конечного t.

Обратим внимание, что порог не меняется при переходе от (a, B, c) к подобной схеме $(P^{-1}a, P^{-1}BP, cP)$. Кроме этого, в определении порога максимальное из чисел $t_1, t_2, \ldots, t_n$ обязательно совпадает с t.

Теорема 3. *Пусть* (a, B, c) *— регулярная схема и* σ *— ее профиль. Порог* frt(a, B, c) *конечен тогда и только тогда, когда профиль* σ *плотен.*

Определение 4. Схема (a, B, c) размерности n над полем $\mathbb{F} = \mathbb{F}_{2^m}$ называется *2-транзитивной*, если найдется натуральное t такое, что для любых двух пар (x, x') и (y, y') различных векторов $\mathbb{F}^n$ выполняется

$$y = (a, B, c)^t [S_1, \ldots, S_t](x),$$
$$y' = (a, B, c)^t [S_1, \ldots, S_t](x')$$

при подходящем выборе $S_1, \ldots, S_t \in S(\mathbb{F})$.

Минимальное t, при котором выполняется данное условие, называется *индексом 2-транзитивности*.

Теорема 4. *Если схема* (a, B, c) *2-транзитивна, то ее профиль плотен.*

Теорема допускает частичное обращение.

Теорема 5. *Пусть* (a, B, c) *— регулярная схема размерности* n*. Если профиль* (a, B, c) *плотен и* $(2^m - 1)^{[n]} \geq 2^{mn} / 2$*, то* ($a$, B, c) *2-транзитивна с индексом, не превосходящем* $2n + \mathrm{frt}(a, B, c) + \mathrm{frt}(a, B, c)^{-1}$.

Пример. *В [4] предложена схема* FourCell*, которая задается следующей матрицей:*

$$\begin{pmatrix} B & a \\ c & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Профиль схемы плотен, frt(a, B, c) = 12, frt(a, B, c)$^{-1}$ = 3 и, следовательно, схема 2-транзитивна с индексом $\leq 2 \cdot 4 + 12 + 3 = 23$.

При этом схема не является сильно регулярной и обосновать ее 2-транзитивность на основании результатов работы [1] не удается.

Библиографические ссылки

1. *Agievich S.* XS-circuits in block ciphers // Mat. Vopr. Kriptogr. 2019. Vol. 10, iss. 2. P. 7–30.

2. *Alfonsin J. L. R.* The Diophantine Frobenius Problem. Oxford University Press, 2005.

3. *Biham E., Biryukov A., Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials // Advances in Cryptology – EUROCRYPT'99 : International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2–6, 1999, Proceedings / ed.: J. Stern. Berlin, Heidelberg : Springer, 1999. P. 12–23. (Lecture Notes in Computer Science, Vol. 1592.)

4. Cryptographic properties and application of a generalized unbalanced Feistel network structure / J. Choy [et al.] // Cryptography and Communications. 2011. Vol. 3, iss. 3. P. 141–164.