7 AES

7.1 AES

Стандарт блочного шифрования AES был принят в США в 2002 году. AES является SQUARE-криптосистемой, $\mathcal{K} \in \{\{0,1\}^{128}, \{0,1\}^{192}, \{0,1\}^{256}\}$, $d \in \{10, 12, 14\}$.

В AES *октеты* (слова длины 8) отождествляются с векторами $\mathbb{F}_2^8$ и элементами поля $\mathbb{F}_{2^8} \cong \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$. Используемый здесь неприводимый многочлен даже получил именное название: *многочлен AES*.

Октеты кодируются числами из $\mathbb{Z}_{2^8}$ в шестнадцатеричной записи. Например:

$$\mathtt{57}_{16} \leftrightarrow (0,1,0,1,0,1,1,1) \leftrightarrow x^6 + x^4 + x^2 + x + 1.$$

Для перемешивания используется матрица размера 4×4. В ячейки матрицы записываются октеты x_{ij}, $0 \leqslant i, j \leqslant 3$. Применяются следующие преобразования:

1. `AddRoundKey`: ко всем октетам одновременно добавляются октеты тактового ключа.

2. `SubBytes`: одновременная замена всех октетов x_{ij} на $S(x_{ij})$. Здесь $S \in S(\{0,1\}^8)$ — S-блок, который действует по правилу:
$$S(x) = A(x^{-1}),$$
где x^{-1} — мультипликативное обращение октета как элемента $\mathbb{F}_{2^8}$ ($0^{-1} = 0$), A — аффинное преобразование x^{-1} как элемента $\{0,1\}^8$.

   S-блок AES задается таблицей: $S(\mathtt{00}_{16}) = \mathtt{63}_{16}$, $S(\mathtt{01}_{16}) = \mathtt{7C}_{16}, \ldots$, $S(\mathtt{FF}_{16}) = \mathtt{16}_{16}$.

3. `ShiftRows`: строка с номером $i = 0, 1, 2, 3$ сдвигается циклически влево на i позиций.

4. `MixColumns`:

   а) каждый из столбцов $(b_0, b_1, b_2, b_3)^{\mathrm{T}}$ связывается с многочленом
   $$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{F}_{2^8}[x];$$

   б) используется фиксированный многочлен
   $$a(x) = \mathtt{03}_{16}x^3 + \mathtt{01}_{16}x^2 + \mathtt{01}_{16}x + \mathtt{02}_{16} \in \mathbb{F}_{2^8}[x];$$

   в) выполняется умножение $a(x)$ на $b(x)$ с последующим нахождением остатка от деления на $x^4 + 1$:
   $$a(x)b(x) = g(x)(x^4 + 1) + b'(x), \quad g, b' \in \mathbb{F}_{2^8}[x], \quad \deg b' < 4;$$

   г) коэффициенты остатка $b'(x)$ определяют результат преобразования `MixColumns`.

   Важно, что $a(x)$ взаимно прост с $x^4 + 1$: имеется многочлен $a^{-1}(x) \in \mathbb{F}_{2^8}[x]$ такой, что $a(x)a^{-1}(x) \equiv 1 \pmod{x^4 + 1}$. Поэтому
   $$b'(x)a^{-1}(x) = b(x)a(x)a^{-1}(x) \equiv 1 \pmod{x^4 + 1},$$
   т.е. обратное преобразование определяется умножением на $a^{-1}(x)$.

При зашифровании выполняются следующие преобразования:

Σ_{1,κ_1}	`AddRoundKey`
	`SubBytes`
	`ShiftRows`
	`MixColumns`

.....	

$\Sigma_{d-1,\kappa_{d-1}}$	`AddRoundKey`
	`SubBytes`
	`ShiftRows`
	`MixColumns`

Σ_{d,κ_d}	`AddRoundKey`
	`SubBytes`
	`ShiftRows`

отбеливание	`AddRoundKey`

Упражнение 7.1. Построить обратные подстановки $\texttt{InvSubBytes} = \texttt{SubBytes}^{-1}$, $\texttt{InvShiftRows} = \texttt{ShiftRows}^{-1}$, $\texttt{InvMixColumns} = \texttt{MixColumns}^{-1}$ и определить преобразование расшифрования. □

7.2 Инверсные S-блоки

Пусть $s \in S(\{0,1\}^n)$ — S-блок. Его задача — разрушать зависимости между обрабатываемыми данными. Существует множество криптографических характеристик S-блоков. Мы рассмотрим одну из них: $R(s)$ — максимальное по ненулевым $\alpha, \beta \in \{0,1\}^n$ число решений уравнения

$$s(x) \oplus s(x \oplus \alpha) = \beta.$$

Чем меньше $R(s)$, тем с меньшим успехом мы можем прогнозировать *выходную разность* $s(x) \oplus s(\tilde{x})$ по *входной разности* $x \oplus \tilde{x}$.

Возникает задача построения s с малыми значениями $R(s)$. В 1993 году Каиса Нюберг предложила решение данной задачи, которое затем часто использовалось во многих криптосистемах, в частности, в AES. Опишем конструкцию Нюберг.

Будем представлять слова из $\{0,1\}^n$ элементами поля $\mathbb{F}_{2^n}$ и, таким образом, перенесем действие s на $\mathbb{F}_{2^n}$, т. е. будем считать, что $s \in S(\mathbb{F}_{2^n})$. Действие s определим следующим образом:

$$s(x) = x^{2^n-2} = \begin{cases} x^{-1}, & x \neq 0, \\ 0, & x = 0. \end{cases}$$

Теорема 7.1. Пусть $s \in S(\mathbb{F}_{2^n})$ — инверсный S-блок. Тогда $R(s) = 4$ при четном n и $R(s) = 2$ при нечетном n.

Доказательство. Пусть $\alpha, \beta \in \mathbb{F}_{2^n}$ и $\alpha \neq 0$. Рассмотрим уравнение

$$s(x+\alpha) - s(x) = \beta \qquad (\star)$$

относительно x. Характеристика $R(s)$ есть максимальное число решений данного уравнения при всевозможных фиксированных α, β. Подсчитаем максимальное число решений. Для этого рассмотрим два случая.

1. Пусть $\beta \neq \alpha^{-1}$. Тогда $x = 0$ и $x = \alpha$ не могут являться решениями $(\star)$. Считая, что $x \notin \{0, \alpha\}$, мы можем записать $(\star)$ в виде:

$$\frac{1}{x+\alpha} + \frac{1}{x} + \beta = \frac{x + (x+\alpha) + \beta x(x+\alpha)}{(x+\alpha)x} = 0$$

и получить эквивалентное квадратное уравнение

$$\beta x^2 + \alpha\beta x + \alpha = 0,$$

которое имеет не более двух решений в поле $\mathbb{F}_{2^n}$.

2. Пусть $\beta = \alpha^{-1}$. В этом случае решениями $(\star)$ являются $x = 0$ и $x = \alpha$, а также, дополнительно, решения уравнения

$$\alpha^{-1}x^2 + \alpha^{-1}\alpha x + \alpha = 0$$

или, что эквивалентно, уравнения

$$x^2 + \alpha x + \alpha^2 = 0.$$

Оценим число решений последнего уравнения. Для этого выполним замену $y = \frac{x}{\alpha}$ и перейдем к уравнению

$$y^2 + y + 1 = 0.$$

Все корни этого уравнения лежат в поле $\mathbb{F}_{2^2}$. Действительно, корнями являются элементы $\lambda, \lambda + 1 \in \mathbb{F}_2[\lambda]/(\lambda^2 + \lambda + 1) \cong \mathbb{F}_{2^2}$.

При четном n поле $\mathbb{F}_{2^2}$ является подполем $\mathbb{F}_{2^n}$, а при нечетном n — нет (почему?). Таким образом, у исходного уравнения $(\star)$ имеется $\leqslant 4$ решений при четном n и $\leqslant 2$ решений при нечетном n, причем верхние границы достижимы. □

7.3 Стратегия «широкого следа»

Стратегия «широкого следа» — это подход к построению линейных преобразований L в SA-криптосистемах, ориентированный на защиту от линейных и разностных атак. Стратегия с успехом применена в AES, стандартах шифрования РФ и Украины.

Будем считать, что прообразы и образы L являются r-векторами над $\mathbb{F}_{2^m}$. Для вектора X его вес Хэмминга $\mathrm{w}(X)$ — это число ненулевых координат. Стратегия «широкого следа» ориентирует на применение L с максимально возможным значением характеристики

$$D(L) = \min_{X \in \mathbb{F}_{2^m}^r \setminus \{0\}} (\mathrm{w}(X) + \mathrm{w}(L(X))).$$

Объясним смысл характеристики на примере разностной атаки. В этой атаке векторы X интерпретируются как разности при обработке двух различных открытых текстов. Пусть $X(t)$ и $Y(t)$ — разности перед и после применения S-блоков на t-м такте, $t = 1, 2, \ldots, d$. Соответствующие координаты $X(t)$ и $Y(t)$ описывают выходные и выходные разности на отдельных S-блоках. Координаты могут быть либо нулевыми либо ненулевыми одновременно. В последнем случае S-блок считается *активным*. Активация S-блока означает, что он преобразует ненулевую разность на входе в ненулевую разность на выходе, при этом выходную разность достаточно трудно спрогнозировать по входной (качество прогнозирования определяется таблицей разностей S-блока). При выборе L стараются добиться, чтобы при обработке любой пары открытых текстов число активных S-блоков было велико.

Искомое число можно оценить следующим образом:

$$\sum_{t=1}^{d} \mathrm{w}(X(t)) = \frac{1}{2}\sum_{t=1}^{d-1}(\mathrm{w}(Y(t) + \mathrm{w}(X(t+1))) + \frac{\mathrm{w}(Y(1)) + \mathrm{w}(X(d))}{2} \geqslant \frac{(d-1)D(L)}{2} + 1.$$

Здесь использованы равенства $\mathrm{w}(X(t)) = \mathrm{w}(Y(t))$ и $X(t+1) = L(Y(t))$.

Вернемся к характеристике $D(L)$. Рассматривая X с весом $\mathrm{w}(X) = 1$, получаем оценку

$$D(L) \leqslant r + 1.$$

Эта оценка достижима, и чтобы продемонстрировать это нам понадобятся элементы теории кодирования.

Множество

$$C = \{(X, L(X)) \colon X \in \mathbb{F}_{2^m}^r\}$$

образует линейный $[2r, r, D(L)]$-код над $\mathbb{F}_{2^m}$. В общем случае *линейный* $[n, k, d]$-*код* над полем K — это линейное подпространство C пространства K^n, которое имеет размерность k и для которого

$$d = \min_{c \in C \setminus \{0\}} \mathrm{w}(c).$$

Параметр n называется *длиной* кода, k — *размерностью*, d — *минимальным расстоянием*. Элементы C — *кодовые слова*.

Теорема 7.2 (граница Синглтона). Для линейного $[n, k, d]$-кода справедлива оценка:

$$d \leqslant n - k + 1.$$

Доказательство. Минимальное расстояние d является также минимальным расстоянием Хэмминга между различными векторами C:

$$\min_{v,v' \in C, v \neq v'} \operatorname{dist}(v, v') = \min_{v,v' \in C, v \neq v'} \mathrm{w}(v + v') = \min_{c \in C, c \neq 0} \mathrm{w}(c) = d.$$

Здесь учтен тот факт, что C является векторным пространством и сумма $v + v'$ обязательно принадлежит C.

Построим новый код C', вычеркивая в векторах C первые $d - 1$ координат. Векторы C отличаются не менее чем в d координатах и поэтому вечеркивание не сократит число векторов: $|C'| = |C| = |K|^k$. С другой стороны, длина C' равняется $n - d + 1$ и, следовательно, $|C'| \leqslant |K|^{n-d+1}$. Таким образом, $|K|^k \leqslant |K|^{n-d+1}$, откуда и следует требуемый результат. □

Линейный код, для которого достигается граница Синглтона, называется *разделимым кодом с максимальным расстоянием* или кратко *кодом МДР* (MDS, от Maximum Distance Separable, в англоязычной литературе).

Примером кодов МДР является коды Рида — Соломона. Они строятся следующим образом: выбираются различные $a_1, a_2, \ldots, a_n \in K$ и множество кодовых слов определяется как

$$C = \{(p(a_1), p(a_2), \ldots, p(a_n)) \colon p \in K[x], \deg p < k\}.$$

Докажем, что минимальное расстояние d этого кода равняется $n - k + 1$. Пусть $p, p' \in K[x]$ — два различных многочлена, степень которых меньше k. Степень $p - p'$ также меньше k, и значения p и p' могут совпасть не более чем в $k - 1$ точках. Следовательно, кодовые слова C отличаются не менее чем в $n - (k - 1)$ координатах, т. е. $d \geqslant n - k + 1$. Оценка достижима, поскольку многочлены $p(x)$ и $p'(x) = p + (x - a_1)(x - a_2) \ldots (x - a_{k-1})$ совпадают ровно в $k - 1$ точке.

Интересующий нас код $\{(X, L(X))\}$ является систематическим — кодируемый вектор X повторяется в кодовом слове. Известно, что для систематических кодов свойство МДР выполняется тогда и только тогда, когда матрица L удовлетворяет одному из следующих требований:

1) любые r столбцов матрицы $[I_r | L]$ линейно независимы (I_r — единичная матрица порядка r);

2) любая квадратная подматрица L обратима (в частности, в L нет нулевых элементов).

При небольших r эти требования можно проверить прямыми расчетами.

Пример 7.1. В AES преобразование `MixColumns` состоит в умножении транспонированного столбца (b_0, b_1, b_2, b_3) на матрицу-циркулянт

$$\begin{pmatrix} \mathtt{02}_{16} & \mathtt{01}_{16} & \mathtt{01}_{16} & \mathtt{03}_{16} \\ \mathtt{03}_{16} & \mathtt{02}_{16} & \mathtt{01}_{16} & \mathtt{01}_{16} \\ \mathtt{01}_{16} & \mathtt{03}_{16} & \mathtt{02}_{16} & \mathtt{01}_{16} \\ \mathtt{01}_{16} & \mathtt{01}_{16} & \mathtt{03}_{16} & \mathtt{02}_{16} \end{pmatrix}.$$

Эта матрица определяет код МДР над $\mathbb{F}_{256}$. Параметры кода: $[8, 4, 5]$. Этот код задает оптимальное линейное перемешивание 4-байтовых столбцов состояния AES (а не всего 16-байтового состояния). □