УДК 519.7 DOI 10.17223/2226308X/11/44

КОМПАКТНАЯ РЕАЛИЗАЦИЯ ФУНКЦИИ ОБРАЩЕНИЯ ЭЛЕМЕНТА В КОНЕЧНОМ ПОЛЕ $\mathbb{F}_{2^{16}}$

И. Е. Кокошинский

Предложено расширение известного метода поиска компактной реализации функции обращения элемента в конечном поле $\mathbb{F}_{2^8}$ на случай поля $\mathbb{F}_{2^{16}}$. Получена верхняя оценка на размер схемы, выполняющей взятие обратного элемента в поле $\mathbb{F}_{2^{16}}$, и доказана теорема о том, что существует реализация функции обращения элемента в поле $\mathbb{F}_{2^{16}}$, использующая для вычисления не больше 336 XOR и 189 AND, или 777 GE.

Ключевые слова: *блочный шифр, поле Галуа, функция обращения элемента в поле Галуа, легковесная криптография, gate equivalent* (*GE*).

Легковесная криптография занимается вопросами компактной реализации шифров и их компонент, в частности S-блоков, главных нелинейных преобразований блочного шифра. S-блок — это, как правило, взаимно однозначная векторная булева функция, которую можно задать как функцию над конечным полем порядка 2^n. Одной из самых простых, но тем не менее криптографически хороших функций для использования в качестве S-блока является функция обращения элемента в поле Галуа. Такая функция является, например, основой S-блока криптосистемы AES.

В [1, 2] предлагается компактная реализация функции обращения над полем $\mathbb{F}_{2^8}$, опирающаяся на идею Винсента Рэймена [3] представления элемента поля как линейного многочлена над полем меньшей размерности и метод Акиры Сато [4], позволяющий ещё более компактно реализовать такую функцию. В данной работе рассматривается расширение данной реализации на поле большей размерности и даётся оценка на размер схемы, выполняющей взятие обратного элемента в поле $\mathbb{F}_{2^{16}}$.

Обращение элементов в поле $\mathbb{F}_{2^n}$ напрямую, как многочленов степени $n-1$ по модулю многочлена степени n, — непростая задача. Но, как показано в [3], обратить элемент как многочлен первой степени по модулю многочлена второй степени сравнительно легко. Для этого представим элемент $g \in \mathbb{F}_{2^n}$ как линейный многочлен от некоторой формальной переменной y над $\mathbb{F}_{2^{n-1}}$:

$$g = \gamma_1 y + \gamma_0, \ \ \gamma_0, \gamma_1 \in \mathbb{F}_{2^{n-1}},$$

с умножением по модулю неприводимого многочлена $r(y) = y^2 + \tau y + \nu$, $\tau, \nu \in \mathbb{F}_{2^{n-1}}$. После перехода к нормальному базису $[Y^{2^{n-1}}, Y]$ поля $\mathbb{F}_{2^n}/\mathbb{F}_{2^{n-1}}$, где $Y, Y^{2^{n-1}}$ — корни $r(y) = y^2 + \tau y + \nu = (y+Y)(y+Y^{2^{n-1}})$, получим

$$g = \gamma_1 Y^{2^{n-1}} + \gamma_0 Y.$$

Тогда $\tau = Y^{2^{n-1}} + Y = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n-1}}}(Y)$ — след, а $\nu = Y^{2^{n-1}} Y = \mathrm{N}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n-1}}}(Y)$ — норма Y. Выразив аналогичным образом элементы поля $\mathbb{F}_{2^{16}}$ через многочлены над $\mathbb{F}_{2^8}$, а элементы этого поля — через многочлены над $\mathbb{F}_{2^4}$ и так далее, можно значительно упростить вычисления и находить обратный элемент в поле $\mathbb{F}_{2^{16}}$ следующим способом.

Утверждение 1. Пусть $x = x_1 K^{256} + x_0 K$, где $x_0, x_1 \in \mathbb{F}_{2^{16}}$; $[K^{256}, K]$ — нормальный базис поля $\mathbb{F}_{2^{16}}/\mathbb{F}_{2^8}$; $t = K^{256} + K$ — след K; $n = K^{256} K$ — норма K. Тогда обратный элемент равен $y = x^{-1} = y_1 K^{256} + y_0 K$, где

$$\begin{aligned} y_1 &= [x_1 x_0 t^2 + (x_1^2 + x_0^2) n]^{-1} x_0, \\ y_0 &= [x_1 x_0 t^2 + (x_1^2 + x_0^2) n]^{-1} x_1. \end{aligned}$$

Можно сделать вычисления ещё более компактными, оптимизируя их схему. Во-первых, можно найти такие неприводимые многочлены, след которых равен единице. Это немного сократит сложность вычислений, поэтому будем считать, что всюду далее след равен единице. Во-вторых, Сато Акира [4] предлагает реорганизовать вычисления так, что возможно вынести часто встречающиеся выражения в отдельные переменные. Здесь и далее $\oplus$ и $\otimes$ обозначают сложение и умножение в поле.

Утверждение 2. Пусть $x \in \mathbb{F}_{2^{16}}$, $x = x_1K^{256} + x_0K$, $x_1, x_0 \in \mathbb{F}_{2^8}$, $[K^{256}, K]$ — нормальный базис поля $\mathbb{F}_{2^{16}}/\mathbb{F}_{2^8}$; $n = K^{256}K$ — норма K. Тогда x^{-1} можно найти следующим образом:

$$
\begin{aligned}
\Psi &= [n \otimes (x_1 \oplus x_0)^2 \oplus (x_1 \otimes x_0)]^{-1},\\
x^{-1} &= [\Psi \otimes x_0]K^{256} + [\Psi \otimes x_1]K.
\end{aligned}
$$

Можно заметить, что часто мы умножаем не два произвольных элемента поля, а некоторый элемент поля на известную константу. Если использовать для этой операции собственную схему и наложить некоторые ограничения на выбор констант, возможна ещё более компактная реализация функции обращения элемента в поле Галуа.

В результате получены оценки сложности вычислений для функции обращения элемента в поле $\mathbb{F}_{2^{16}}$ и всех её составляющих.

Теорема 1. Существует реализация функции обращения элемента в поле $\mathbb{F}_{2^{16}}$, использующая для вычисления не больше 336 XOR и 189 AND, или 777 GE.

ЛИТЕРАТУРА

1. *Canright D.* A Very Compact Rijndael S-box. Naval Postgraduate School Technical Report: NPS-MA-05-001, 2004.
2. *Canright D.* A very compact S-box for AES // LNCS. 2005. V. 3659. P. 440–455.
3. *Rijmen V.* Efficient Implementation of the Rijndael S-box. Katholieke Universiteit Leuven, Dept. ESAT, Belgium, 2001.
4. *Satoh A., Morioka S., Takano K., and Munetoh S.* A compact Rijndael hardware architecture with S-box optimization // ASIACRYPT 2001. LNCS. 2001. V. 2248. P. 239–254.