7. *Bogart C.* Calculating Frobenius numbers with Boolean Toeplitz matrix multiplication // For Dr. Cull, CS 523, March 17, 2009. Oregon State University.
8. *Nijenhuis M.* A minimal-path algorithm for the "money changing problem" // The American Mathematical Monthly. 1979. V. 86. P. 832–835.
9. *Bocker S. and Liptak Z.* The "money changing problem" revisited: computing the Frobenius number in time $O(ka_1)$. Technical Report No. 2004-2, Univ. of Bielefeld, Technical Faculty, 2004.

УДК 519.7

ИТЕРАТИВНАЯ КОНСТРУКЦИЯ APN-ФУНКЦИЙ[1]

А. А. Фролова

Векторные булевы функции F и G назовём γ-эквивалентными, если для каждой пары векторов $a \neq 0$, b уравнения $F(x) \oplus F(x \oplus a) = b$ и $G(x) \oplus G(x \oplus a) = b$ одновременно имеют или не имеют решений. Установлено, что все классы γ-эквивалентности APN-функций от n переменных имеют мощность 2^{2n}. Предложена итеративная конструкция APN-функций.

Ключевые слова: *векторная булева функция, APN-функция, γ-эквивалентность, итеративная конструкция.*

Булевой функцией от n переменных называется любое отображение $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. *Весом Хэмминга* $\mathrm{wt}(f)$ булевой функции f называется количество единиц в векторе её значений. *Векторной булевой функцией* F называется любое отображение $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$. Векторную функцию можно рассматривать как набор из m координатных булевых функций от n переменных, т. е. $F = (f_1, \ldots, f_m)$.

Булевы функции, использующиеся в криптографических приложениях, должны обладать рядом специальных свойств для обеспечения стойкости к некоторым видам криптоанализа. В работе [1] определено следующее требование к функции. Векторная функция F называется *δ-дифференциально равномерной*, если для любых векторов $a \neq 0$, b уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений. Для обеспечения стойкости шифра к дифференциальному криптоанализу необходимо использовать δ-дифференциально равномерные векторные булевы функции с малым значением δ.

Далее рассматриваем только случай $n = m$. В этом случае минимальное возможное δ равно двум. *APN-функцией* (Almost Perfect Nonlinear) называется 2-дифференциально равномерная векторная функция. В работе [2] приведён обзор по известным APN-функциям. Открытыми вопросами остаются оценки количества и новые способы построения APN-функций.

Пусть $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. Для F и любого вектора $a \neq 0$ определяется множество

$$B_a(F) = \{F(x) \oplus F(x \oplus a) : x \in \mathbb{Z}_2^n\}.$$

Для F строится булева функция γ_F от $2n$ переменных следующим образом:

$$\gamma_F(a, b) = \begin{cases} 1, & \text{если } a \neq 0 \text{ и } b \in B_a(F), \\ 0 & \text{иначе.} \end{cases}$$

Известно, что F — APN-функция тогда и только тогда, когда $\mathrm{wt}(\gamma_F) = 2^{2n-1} - 2^{n-1}$.
Пусть $F, F' : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$.

[1]Работа поддержана грантом РФФИ, проект № 12-01-31097.

Определение 1. Функции F и F' назовём *γ-эквивалентными*, если $\gamma_F = \gamma_{F'}$.

Нетрудно убедиться, что γ-эквивалентность является отношением эквивалентности на множестве всех векторных булевых функций. Следовательно, множество функций распадается на непересекающиеся классы.

Получены следующие результаты.

Теорема 1. Пусть F — APN-функция от n переменных. Тогда все функции $F_{c,d}(x) = F(x \oplus c) \oplus d$, где $c, d \in \mathbb{Z}_2^n$, являются APN-функциями, γ-эквивалентными F. Кроме того, все функции $F_{c,d}$ попарно различны.

Теорема 2. Пусть γ — булева функция от $2n$ переменных, $\gamma = \gamma_F$ для некоторой APN-функции F от n переменных. Тогда существует не более 2^{2n} APN-функций с такой γ.

Следствие 1. В каждом классе γ-эквивалентности APN-функций от n переменных ровно 2^{2n} различных функций.

Опишем итеративную конструкцию APN-функции от $n+1$ переменных из двух APN-функций и двух булевых функций от n переменных.

Теорема 3. Пусть F и G — APN-функции от n переменных, f и g — булевы функции от n переменных. Пусть S — векторная булева функция от $n+1$ переменных, определённая как

$$S(x, x_{n+1}) = ((x_{n+1} \oplus 1)F(x) \oplus x_{n+1}G(x),\ (x_{n+1} \oplus 1)f(x) \oplus x_{n+1}g(x)),$$

где $x \in \mathbb{Z}_2^n$, $x_{n+1} \in \mathbb{Z}_2$. Тогда S — APN-функция, если выполнено условие

$$\begin{gathered}\text{для всех } x, y, a \in \mathbb{Z}_2^n, a \neq 0, \text{таких, что } F(x) \oplus F(x \oplus a) = G(y) \oplus G(y \oplus a),\\ \text{выполняется } f(x) \oplus f(x \oplus a) \neq g(y) \oplus g(y \oplus a).\end{gathered} \tag{1}$$

Следствие 2. Пусть F и G — APN-функции от n переменных, f и g — булевы функции от n переменных, удовлетворяющие условию (1). Тогда функции $F'(x) = F(x \oplus c') \oplus d'$, $G'(x) = G(x \oplus c'') \oplus d''$, $f' = f(x \oplus c') \oplus d_1$, $g'(x) = g(x \oplus c'') \oplus d_2$ удовлетворяют условию (1) для любых $c', c'', d', d'' \in \mathbb{Z}_2^n$, $d_1, d_2 \in \mathbb{Z}_2$.

Открытым остаётся вопрос, как выбрать APN-функции F, G и булевы функции f, g, которые бы удовлетворяли условию (1). При малых n экспериментально показано, что для любой APN-функции F найдётся достаточно много функций G, f, g, удовлетворяющих (1). Можно сформулировать гипотезу.

Гипотеза 1. Для любой APN-функции F от n переменных найдутся APN-функция G и булевы функции f, g от n переменных, удовлетворяющие условию (1).

ЛИТЕРАТУРА

1. *Nyberg K.* Differentially uniform mappings for cryptography // Eurocrypt 1993. LNCS. 1994. V. 765. P. 55–64.
2. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.