

С. М. Сулгин, О. А. Финько (Краснодар, КВВУ (ВИ)). **Контроль ошибок логических вычислений на основе синтеза избыточных арифметико-логических АН-форм.**

При реализации логических функций криптографических алгоритмов именно методы функционального диагностирования соответствуют специфике решаемых средствами шифрования задач, т. к. препятствуют компрометации шифров в реальном масштабе времени. Реализация систем булевых функций (БФ) посредством арифметико-логических форм (АЛФ) обеспечивает преимущества по распараллеливанию и повышению гибкости логических вычислений [1]. Однако за рамками известных публикаций остались вопросы синтеза избыточных АЛФ, обладающих свойствами помехоустойчивых кодов.

Введем отображение матрицы истинности $\mathbf{Y}$ системы БФ $f_1(X), f_2(X), \dots, f_d(X)$ от переменных $X = x_1, x_2, \dots, x_n$ в матрицу истинности $\mathbf{Q}$, в которой значения $(q_{d+s}^{(i)} \dots q_1^{(i)})_2$, принимаемые реализуемыми БФ на i -м наборе переменных, являются словами избыточного арифметического АН-кода:

$$\begin{pmatrix} \mathbf{Y}_d & \mathbf{Y}_{d-1} & \dots & \mathbf{Y}_1 \\ y_d^{(0)} & y_{d-1}^{(0)} & \dots & y_1^{(0)} \\ y_d^{(1)} & y_{d-1}^{(1)} & \dots & y_1^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ y_d^{(2^n-1)} & y_{d-1}^{(2^n-1)} & \dots & y_1^{(2^n-1)} \end{pmatrix} = \begin{pmatrix} \mathbf{Y} \\ Y^{(0)} \\ Y^{(1)} \\ \vdots \\ Y^{(2^n-1)} \end{pmatrix} \Rightarrow$$

$$\begin{pmatrix} \mathbf{Q}_{d+s} & \dots & \mathbf{Q}_d & \dots & \mathbf{Q}_1 \\ q_{d+s}^{(0)} & \dots & q_d^{(0)} & \dots & q_1^{(0)} \\ q_{d+s}^{(1)} & \dots & q_d^{(1)} & \dots & q_1^{(1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ q_{d+s}^{(2^n-1)} & \dots & q_d^{(2^n-1)} & \dots & q_1^{(2^n-1)} \end{pmatrix} = \begin{pmatrix} \mathbf{Q} \\ Q^{(0)} \\ Q^{(1)} \\ \vdots \\ Q^{(2^n-1)} \end{pmatrix},$$

где $y_j^{(i)}$ — значения, принимаемые j -й БФ на i -м наборе переменных, $Y^{(i)}$ — целые неотрицательные числа, записанные в двоичной системе счисления: $Y^{(i)} = (y_d^{(i)} y_{d-1}^{(i)} \dots y_1^{(i)})_2 = \sum_{j=1}^d y_j^{(i)} 2^{j-1}$; s — количество избыточных БФ.

Например, для неразделимого АН-кода, порождаемого генератором A ($A > 1$ — нечетное число) получим: $\mathbf{Y} \rightarrow A\mathbf{Y} = \mathbf{Q}$, где $\mathbf{Q}$ — кодовое слово и $A\mathbf{Y} = [A\mathbf{Y}_d | A\mathbf{Y}_{d-1} | \dots | A\mathbf{Y}_1]^T$, $\mathbf{Q} = A\mathbf{Y} = [Q_{d+s} | \dots | Q_d | \dots | Q_1]^T = [Q^{(0)} Q^{(1)} \dots Q^{(2^n-1)}]^T$, $Q^{(i)} = (q_{d+s}^{(i)} \dots q_d^{(i)} \dots q_1^{(i)})_2 = \sum_{j=1}^{d+s} q_j 2^{j-1}$ — целое неотрицательное число, T — символ транспонирования.

Избыточную АН-АЛФ получим путем *прямого* конъюнктивного преобразования:

$$\mathbf{B} = \mathbf{A}_{2^n} \mathbf{Q}, \quad (1)$$

где $\mathbf{A}_{2^n}$ — матрица прямого арифметического преобразования размерности $2^n \times 2^n$, $\mathbf{B} = [\beta_0 \beta_1 \dots \beta_{2^n-1}]^T$ — вектор коэффициентов полинома, реализующего систему БФ:

$$Q(X) = \sum_{i=0}^{2^n-1} \beta_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \quad \beta_i \in \mathbf{Z}, \quad i = 0, 1, \dots, 2^n - 1,$$

$$(i_1 i_2 \dots i_n)_2 = \sum_u^n i_u 2^{n-u} \quad (i_u \in \{0, 1\}), \quad x_u^{i_u} = \begin{cases} x_u, & \text{если } i_u = 1, \\ 1, & \text{если } i_u = 0. \end{cases}$$

Противоположным преобразованию (1) является *обратное* конъюнктивное преобразование: $\mathbf{Q} = \mathbf{A}_{2^n}^{-1} \mathbf{B}$. В процессе реализации систем БФ выполняется классиче-

ская процедура декодирования [2] (преобразование вектора $\mathbf{Q} \rightarrow \mathbf{Y}$) AN -кода с контролем ошибок логических вычислений в соответствии со свойствами и выбранными параметрами AN -кода.

СПИСОК ЛИТЕРАТУРЫ

1. *Финько О. А.* Модулярная арифметика параллельных логических вычислений: М.: Ин-т проблем управления им. В. А. Трапезникова РАН, 2003, 224 с.
2. *Дадаев Ю. Г.* Арифметические коды, исправляющие ошибки. М: Советское радио, 1969, 168 с.