ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 26 МАТЕМАТИКИ Выпуск 2
2019

**Е. В. Кутырёва** (Москва, ТВП). **К вопросу о параметрах одного алгоритма итерационного декодирования.**

В итерационных алгоритмах декодирования построенные проверочные соотношения соответствующего кода используются для исправления искаженного кодового слова и получения нового слова, на каждой итерации всё более близкого к исходному кодовому слову (см. [1, 2]).

Рассмотрим генератор гаммы, состоящий из РСЛОС длины $L$ с характеристическим многочленом $g(x)$ и некоторой функции усложнения. Каждый участок выходной последовательности РСЛОС длины $L$ можно рассматривать как кодовое слово двоичного линейного кода $C$ длины $L$ и размерности $N$. Тогда соответствующий участок гаммы длины $N$ можно рассматривать как кодовое слово, переданное по двоичному симметричному каналу, где каждый символ искажается с вероятностью $p < \frac{1}{2}$ и передается без искажения с вероятностью $1-p$.

Опишем в общем виде алгоритм итерационного декодирования (см. [1, 3]).

Определим $k$-член $q(x)$, кратный характеристическому многочлену $g(x)$,

$$q(x) = 1 \oplus x^{i_1} \oplus \cdots \oplus x^{i_{k-1}}.$$

Выполняется соотношение $b_{i+i_1} \oplus b_{i+i_2} \oplus \cdots \oplus b_{i+i_{k-1}} = x_i \oplus \varepsilon_{i+i_1} \oplus \varepsilon_{i+i_2} \oplus \cdots \oplus \varepsilon_{i+i_{k-1}}$. Здесь $x_i$, $i = \overline{1,N}$ — знаки выходной последовательности РСЛОС, $b_i$, $i = \overline{1,N}$ — наблюдения над ними (знаки гаммы), $\varepsilon_i$, $i = \overline{1,N}$ — искажения.

Соотношения $x_i = x_{i+i_1} \oplus x_{i+i_2} \oplus \cdots \oplus x_{i+i_{k-1}}$, $1 \leqslant i + i_j \leqslant t$, построенные с помощью $k$-члена $q(x)$, будем называть $k$-членными (проверочными) соотношениями, ассоциированными с последовательностью $x_i$. Обозначим через $m_k(i)$ число таких соотношений, которые можно использовать при количестве материала $N \ll 2^L - 1$.

Через $m_{0,k}(x_i)$ обозначим мощность следующего множества

$$\{(i_1, \ldots, i_{k-1}),\ 1 \leqslant i_1 \leqslant \cdots \leqslant i_{k-1} \leqslant N,\ 1 \leqslant i + i_j \leqslant N | \\ g(x) | q(x), b_{i+i_1} \oplus b_{i+i_2} \oplus \cdots \oplus b_{i+i_{k-1}} = 0\}.$$

По наблюдаемому набору значений $m_{0,k}(x_i)$, $3 \leqslant k \leqslant d$, $d \ll N$, будем определять значение $x_i$, подсчитав апостериорную вероятность того, что $x_i$ принимает фиксированное значение. Обозначим через $m \geqslant 3$ минимальное значение $k$ такое, что $N_k(i) = 1$. Пусть $\widehat{\Delta} = 2p - 1$.

**Алгоритм**

1. Устанавливаем номер итерации алгоритма $r = 0$.
2. Для $i = \overline{1,N}$
   (a) Подсчитываем величину $S(r) = \frac{1}{2} \sum_{k=m}^{d} m_k(i) \operatorname{arg\,tanh}((-1)^k \widehat{\Delta}^{k-1})$.
   (b) Подсчитываем величину $S_1(r) = \sum_{k=m}^{d} m_{0,k}(x_i) \operatorname{arg\,tanh}((-1)^k \widehat{\Delta}^{k-1})$.
   (c) Если $S_1(r) \geqslant S(r)$, $x_i(r) = 1$, в противном случае $x_i(r) = 0$. При $r = 1$ переходим к п.2.4, в противном случае — к п.2.1.

Если $\widehat{\Delta}_i(1) \geqslant \widehat{\Delta}_i$, алгоритм заканчивает работу, на выходе — неуспех, в противном случае переходим к п.2.1.

3. Выполняем присваивание $b_i = x_i(r)$, $i = \overline{1, N}$. Увеличиваем номер итерации на единицу. Переходим к п. 2.

Не умаляя практической значимости описанного алгоритма, следует отметить, что при переоценке вероятности значения $x_i$ в данном алгоритме используются полиномы, которые могут иметь другие общие неизвестные, кроме $x_i$. Это приводит к получению неверных оценок апостериорной вероятности искажения $x_i$, и, как следствие, к искажению теоретических оценок для данного алгоритма, например, может занижаться количество требуемого для решения задачи материала.

**Утверждение 1.** Среднее число $E(l)$ различных переменных в множестве полиномов степени $d$, $d > 3$, кратных полиному $P(x)$, образующих ортогональную систему относительно неизвестного $x_i$, вычисляется по следующей формуле $\sum\limits_{k=d-2+m_d(i)}^{(d-1)m_d(i)} Pl = k \cdot k$, его можно оценить снизу величиной $(d-1) \cdot m \prod\limits_{k=1}^{m_d(i)-1} \frac{\binom{N-1-k(d-1)}{d-1}}{\binom{N-1}{d-1}-k}$.

**Утверждение 2.** *Среднее число полиномов степени* $d$, $d > 3$, *кратных полиному* $P(x)$, *образующих ортогональную систему относительно неизвестного* $x_i$, *ее можно оценить величиной* $\frac{E(l)}{d-1}$

$$\frac{1}{d-1} \sum_{k=d-2+m_d(i)}^{(d-1)m_d(i)} \frac{k \cdot \binom{N-1}{k}(N - \lceil \frac{k}{m} \rceil)^{m_d(i)-k \bmod m_d(i)} \left(\binom{N-\lceil \frac{k}{m} \rceil - 1}{d-\lceil \frac{k}{m} \rceil - 1}(d - \lceil \frac{k}{m} \rceil - 1)!\right)^{m_d(i)}}{\binom{N-1}{m_d(i)}\left(\binom{N-2}{d-1}(d-1)!\right)^{m_d(i)}}.$$

## СПИСОК ЛИТЕРАТУРЫ

1. *Canteaut A., Trabbia M.* Improved fast correlation attacks using parity-check equations of weights 4 and 5. Advances in cryptology – Eurocrypt'00, V. 1807 of Lecture notes in computer science, Springer Verlag, 2000, p. 573–588.
2. *Meier W., Staffelbach O.* Fast correlation attack on certain stream ciphers. — Journal of cryptology, 1989, v. 1, p. 159–176.
3. *Mitton M.* An analysis and an improvement of iterative fast correlation attacks. — Journal of Discrete Mathematical Science and Cryptography, 2005.