УДК 004.4

МАТРИЧНОЕ УМНОЖЕНИЕ НАД ПОЛЕМ GF(2) В ЗАЩИТЕ БЕСПРОВОДНЫХ КАНАЛОВ СИСТЕМ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ

В. В. Скуратов,
начальник военной кафедры
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Рассмотрены особенности применения метода логических преобразований, основанного на матричном умножении в поле GF(2), для защиты беспроводных каналов систем управления робототехническими комплексами от помех, перехвата и искажения информации. Показано, что реализация данного метода не требует перестройки оборудования и программного обеспечения, хорошо согласуется с кодированием и декодированием сообщений, обеспечивает обнаружение и исправление ошибок, возникающих в канале связи, а также решение задач распределенного доступа.

Ключевые слова *— преобразование информационных потоков, матричное умножение в поле GF(2), построение матриц над полем GF(2).*

В настоящее время для решения задач мониторинга территорий и объектов все чаще находят применение автономные роботы и робототехнические комплексы, оснащенные различными датчиками, средствами наблюдения, навигации, связи и вооружением. Для управления роботами, обеспечения взаимодействия их между собой, а также обмена разнородной информацией с пунктом управления используются каналы радиосвязи. Радиоканал является наиболее уязвимым элементом робототехнического комплекса. Действия возможного нарушителя, направленные на создание различного рода помех, получение доступа к информации обмена или к контуру управления создадут условия, при которых выполнение возложенных на комплекс задач станет трудновыполнимым или невозможным [1].

Для предупреждения подобных нарушений необходимы универсальные, эффективные и в то же время экономичные аппаратные и программные средства преобразования информационных потоков, обеспечивающие достоверность, целостность, скрытность и высокую скорость обмена информацией.

Реализуемые методы преобразования информации должны быть универсальны и обеспечивать функционирование системы при формировании и передаче команд управления подвижными объектами, телеметрической и другой полезной информации, поступающей от объекта управления, в том числе речевой, телекодовой, текстовой, аудио- и видеоизображений без потери в скорости обработки и передачи данных [2, 3].

Существующие сегодня средства защиты каналов обмена характеризуются использованием значительных вычислительных ресурсов, что существенно снижает скорость обмена данными в системе управления. Реализация средств защиты программными и аппаратными средствами требует значительных затрат на создание спецпроцессоров и увеличения массогабаритных характеристик.

В качестве одного из методов, удовлетворяющих перечисленным выше требованиям, целесообразно использовать метод преобразования информационных потоков, основанный на матричном умножении в поле GF(2). Реализация данного преобразования не требует перестройки оборудования и программного обеспечения, хорошо согласуется с кодированием и декодированием сообщений, обеспечивает обнаружение и исправление ошибок, возникающих в канале связи, а также решение задач распределенного доступа [1].

Рассмотрим матрицы размера (n, n) с элементами $\{0, 1\}$. Число таких матриц равно 2^{n^2}. Исключим из множества этих матриц все матрицы с определителем, равным 0 (в поле Галуа GF(2)). Результат перемножения произвольных матриц

размера (n, n) с определителем, равным 1, является матрица с определителем, равным 1, т. е. множество таких матриц замкнуто относительно операции умножения в поле GF(2) [4].

Для построения матриц над полем GF(2) произвольных размеров предложен алгоритм, который позволяет по матрице размера (n, n) строить матрицу размера $(n + 1, n + 1)$, и на основании этого алгоритма показано, что число матриц размера (n, n) с определителем, равным 1, можно найти по формуле

$$N = (2^n - 1)(2^{n-1} - 1)...3 \cdot 2^{n(n-1)/2}. \qquad (1)$$

Для удобства будем пользоваться нижней оценкой количества матриц в виде степени числа 2. Эту оценку количества матриц размера (n, n) с определителем, равным 1, можно получить следующим образом.

Рассмотрим произведение $P = (2^n - 1)(2^{n-1} - 1)...(2^2 - 1)$.

Перемножим в общем виде члены этого произведения и оставим только первые три старших члена. Если обозначить через $R = n + (n - 1) + (n - 2) + ... + 3 + 2 = (n^2 + n - 2)/2$, то первые три старших члена будут иметь вид $2^R - 2^{R-2} - 2^{R-3}...$. Последующие члены будут иметь знаки как «+», так и «−», но их степени будут убывать, поэтому P будет находиться в пределах $2^R > (2^n - 1)(2^{n-1} - 1)...(2^2 - 1) > 2^{R-1}$.

За нижнюю оценку можно принять 2^{R-1}. Тогда нижняя оценка числа матриц размера (n, n) с определителем, равным 1, будет определяться по условию $N > 2^{n^2-2}$.

Полученный результат позволяет легко оценить сложность алгоритма подбора матрицы, а следовательно, и качество кодирования информации.

Для размера матриц (20, 20) нижняя оценка дает 2^{398}. Используя очевидную оценку $2^{10} > 10^3$, получаем, что число матриц размера (20, 20) с определителем, равным 1, превышает величину $2{,}5 \cdot 10^{119}$.

Кодирование и декодирование информации с использованием матриц с определителем 1 в поле GF(2) может выполняться различными способами.

Во-первых, путем умножения матрицы **M** слева на столбец, составленный из фрагментов сообщения, т. е. $\mathbf{M} \times \mathbf{Q} = \mathbf{L}$, где **Q** — исходное сообщение, **L** — кодированное сообщение. Декодирование сообщения может выполняться путем умножения **L** слева на матрицу $\mathbf{M}^{-1}$, действительно: $\mathbf{M}^{-1} \times \mathbf{L} = \mathbf{M}^{-1} \times \mathbf{M} \times \mathbf{Q} = \mathbf{Q}$.

При другом способе кодированное сообщение **L** нужно транспонировать (из столбца превратить в строку) и умножить справа на матрицу, обратную к транспонированной матрице **M**. Действительно, так как $(\mathbf{M} \times \mathbf{Q})^T = \mathbf{L}^T = \mathbf{Q}^T \times \mathbf{M}^T$, то $\mathbf{Q}^T = \mathbf{L}^T(\mathbf{M}^T)^{-1}$.

Оба способа кодирования информации являются эквивалентными по сложности, но могут комбинироваться в целях увеличения достоверности полученной информации.

Еще одно важное свойство метода кодирования с использованием матриц в поле Галуа состоит в том, что после кодирования любой последовательности символов результат выглядит как случайная последовательность.

Пусть имеется последовательность из 1 и 0 со смещенной вероятностью единиц и нулей и пусть вероятность появления 1 в этой последовательности равна p, а нуля, соответственно, $1 - p$. Выберем произвольную пару символов этой последовательности и сложим их по mod2. Вероятность появления 1 в результирующей последовательности будет равна $P(1) = 2p(1 - p)$, а нуля, соответственно, $1 - 2p(1 - p)$. Возьмем теперь три произвольных бита последовательности и сложим их по mod2. Тогда вероятность появления 1 в результирующей последовательности будет равна $3p(1 - p)^2 + p^3$. Применяя данный подход, построим таблицу оценки матриц в поле GF(2).

Формула, приведенная в таблице, использует свойство функции сложения по mod2 n аргументов. Функция равна 1 на тех наборах в ее таблице истинности, в которых число аргументов, прини-

■ Оценка матриц в поле GF(2)

n	$P(1)$	$P(1)$ при $p = 0{,}9$	Модуль разности $P(1) - 0{,}5$
1	p	0,9	0,4
2	$2p(p - 1)$	0,18	0,32
3	$3p(1 - p)^2 + p^3$	0,756	0,256
4	$4p(1 - p)^3 + 4p^3(1 - p)$	0,2952	0,2048
5	$5p(1 - p)^4 + 10p^3(1 - p)^2 + p^5$	0,66384	0,16384
6	$6p(1 - p)^5 + 20p^3(1 - p)^3 + 6p^5(1 - p)$	0,368928	0,131072
7	$7p(1 - p)^6 + 35p^3(1 - p)^4 + 21p^5(1 - p)^2 + p^7$	0,60485193	0,10485193
8	$8p(1 - p)^7 + 56p^3(1 - p)^5 + 56p^5(1 - p)^3 + 8p^7(1 - p)$	0,41611392	0,08388608
9	$9p(1 - p)^8 + 84p^3(1 - p)^6 + 126p^5(1 - p)^4 + 36p^7(1 - p)^2 + p^9$	0,567108864	0,067108864
n	$P(1) = \sum_{k=0}^{s} C_n^{2k=1} p^{2k+1} \times \times (1-p)^{n-(2k+1)}$, где $s = \left\lfloor \frac{n-1}{2} \right\rfloor$; $[x]$ — округление до целого в меньшую сторону		

мающих значение 1, нечетно, и 0 на всех остальных наборах.

Выведенная формула будет использована для оценки характеристик построенных матриц с определителем 1 в поле GF(2).

Правый столбец таблицы показывает, что даже при большой асимметрии последовательности ($p = 0{,}9$) после девятикратного сложения битов по mod2 результирующая последовательность становится практически квазислучайной ($P(1)$ и $P(0) \approx 0{,}5$).

Произведена оценка скорости кодирования/декодирования с помощью матриц над полем GF(2) и дана оценка качества этого метода.

Пусть длина сообщения в битах равна $L = kn$, где k — размер блока в битах; (n, n) — размер матрицы кодирования или декодирования.

Эксперименты с построением матриц с хорошими кодирующими свойствами показали, что в таких матрицах число единиц в каждой строке примерно равно числу нулей, т. е. $\approx n/2$. Тогда число операций сложения по mod2 блоков равно $\frac{i^2}{2}$. Число операций на 1 бит сообщения равно $\frac{n^2}{2} \Big/ kn = \frac{n^2}{2kn} = \frac{n}{2k}$.

Таким образом, чем меньше размер матрицы n и больше размер блока кодируемого сообщения, тем меньше приходится простых операций на бит информации. При размере матрицы (20, 20) и $k = 5$ число операций на бит равно 2. При размере матрицы (128, 128) и $k = 16$ число операций на бит равно 16. Однако при увеличении размера матриц должна увеличиваться надежность кодирования.

При использовании для шифрования матриц, которые порождают циклические группы больших порядков, возможно решать задачи адресной передачи сообщений, когда передаваемое сообщение может быть декодировано только конкретным адресатом. Такая ситуация возникает при управлении большим количеством автономных объектов.

Рассмотрим ситуацию, когда из единого центра нужно передавать сообщения разным абонентам, причем так, что если сообщение адресовано клиенту с номером i, то клиент с номером j ($i \neq j$) не смог бы прочитать это сообщение [5]. Пусть имеется k адресатов.

Порядок циклической группы, порождаемой матрицей **M**, пусть равен s. Пусть s — евклидово число, т. е. число, каноническая форма которого имеет вид $s = p_1p_2p_3...p_k$. Снабдим i-го адресата матрицей вида $\mathbf{M}^{p1p2p3...pk\ -\ pi}$. Для передачи T i-му адресату сообщения кодирование его осуществим путем умножения слева на матрицу $\mathbf{M}^{pi}$. Таким образом декодируя полученное сообщение, i-й адресат точно восстановит его, умножив слева кодированное сообщение на матрицу $\mathbf{M}^{p1p2p3...pk\ -\ pi}$.

Ни один из других адресатов не сможет правильно декодировать передаваемое сообщение. Пусть, например, j-й адресат попытается декодировать это сообщение. Он умножит закодированное сообщение слева на матрицу $\mathbf{M}^{p1p2p3...pk\ -\ pj}$, в результате чего получит $\mathbf{M}^{p1p2p3...pk\ -\ pj} \times \mathbf{M}^{pi} \times \mathbf{T}$, т. е. бессмысленный набор символов. Однако он может попытаться проделать умножение с помощью матрицы, которой владеет, несколько раз в надежде на каком-то шаге вскрыть сообщение. Но это не произойдет, так как необходимо, чтобы на шаге t выполнилось сравнение $(p_1p_2p_3...p_k - p_j)^t \equiv \equiv p_i \bmod (p_1p_2p_3...p_k)$. Но это сравнение не имеет решения, поскольку в правой части стоит член, который не является взаимно простым с модулем $p_1p_2p_3...p_k$ [4, 5].

Таким образом, использование методов матричного умножения над полем GF(2) представляется вполне эффективным при решении задач преобразования информационных потоков, выявлении и устранении ошибок распределенного доступа. Данные методы обладают высокой скоростью кодирования информации, относительно простой реализуемостью программно-аппаратными средствами.

Литература

1. **Скуратов В. В.** Использование логических преобразований для защиты информационных потоков в робототехнических комплексах, осуществляющих мониторинг состояния окружающей среды и территорий // Актуальные вопросы разработки и внедрения информационных технологий двойного применения: тез. докл. VI Всерос. науч.-практ. конф., 12–14 октября 2005 г., Ярославль, 2005. С. 102–104.
2. **Бубликов А. Б., Ерош И. Л., Сергеев М. Б.** Особенности использования булевых функций для организации криптографических преобразований потоковой информации // Информационно-управляющие системы. 2003. № 6. С. 54–57.
3. **Балонин Ю. Н., Востриков А. А., Сергеев М. Б.** О прикладных аспектах применения М-матриц // Информационно-управляющие системы. 2012. № 1. С. 92–93.
4. **Ерош И. Л., Скуратов В. В.** Адресная передача сообщений с использованием матриц над полем GF(2) // Проблемы информационной безопасности. 2004. № 1. С. 72–78.
5. **Скуратов В. В.** Защищенные пароли // Искусственный интеллект. Интеллектуальные и многопроцессорные системы-2004: материалы Междунар. науч. конф. / ТРТУ. Таганрог, 2004. Т. 1. С. 350–353.