УДК 681.391.1

ЗАЩИТА ИНФОРМАЦИОННЫХ ПОТОКОВ В СИСТЕМАХ РАСПРЕДЕЛЕННОГО КОНТРОЛЯ И УПРАВЛЕНИЯ

И. Л. Ерош,
д-р техн. наук, профессор
Санкт-Петербургский государственный университет аэрокосмического приборостроения (СПбГУАП)

Рассмотрена проблема защиты информации в распределенных системах контроля и управления. В этих задачах число объектов контроля и управления может составлять сотни тысяч единиц, а в перспективе — и миллионы. Отмечено, что классические криптосистемы в таких применениях обладают рядом недостатков из-за своей сложности и не обеспечивают реального масштаба времени. Обсуждается вопрос использования простых методов защиты, основанных на преобразовании управляющих, контролирующих и ответных сигналов с помощью булевых преобразований. Отмечается преимущество такого подхода в ряде перспективных приложений.

Историческая справка

В начале 70-х годов прошлого века среди программистов была популярна игра «Жизнь». В этой игре к элементам двоичной матрицы A размера $n \times n$ применялась некоторая функция F, с помощью которой строилась матрица B того же размера. Чаще всего в таких преобразованиях использовалась функция американского математика Конвея [1]. Функция Конвея задавалась следующим образом. Каждый элемент b_{ij} матрицы B являлся результатом применения функции Конвея к соответствующим элементам a_{ij} матрицы A и некоторым элементам из ближайшего окружения a_{ij}. Так, если $a_{ij} = 0$, то и $b_{ij} = 0$. Если же $a_{ij} = 1$, то $b_{ij} = 1$, если в ближайшем окружении a_{ij} ровно два или три элемента принимали значение 1, в противном случае $b_{ij} = 0$. Применение такого преобразования с функцией Конвея приводило к удивительным преобразованиям двоичных изображений: изображения смещались, вращались, распадались на несколько новых конфигураций, частично стирались и т. п. В одном из университетов Англии в качестве исходного изображения (матрицы A) было взято изображение, отдаленно напоминающее мордочку кота и названное «Чеширским котом» [1]. Применяя многократно преобразование с функцией Конвея к изображению «Чеширского кота», авторы получили ряд картин, которые можно было интерпретировать как пропадание изображения кота, — оно превращалось в изображение, похожее на «улыбку» (вспомните сказку Л. Кэррола «Алиса в стране чудес» и то, как кот уходил, оставляя на некоторое время в комнате свою улыбку). При очередном применении преобразования с функцией Конвея «улыбка» превращалась в устойчивую конфигурацию «лапка». Дальнейшее применение преобразований с функцией Конвея уже не меняло изображение «лапки».

В эти же годы автор активно занимался автоматизацией технологических операций на различных производствах: фарфорофаянсовом заводе, хлебозаводах, птицефабриках, приборостроительных производствах, автомобильных и тракторных производствах. На всех этих предприятиях при внедрении роботехнических комплексов с простейшим техническим зрением или осязанием требовалось решать задачи обработки двухградационных изображений с целью учета продукции на конвейерах, сортировки по размерам и форме, автоматического адресования, изменения программ обработки, в частности, окраски, сварки и т. п. Именно тогда родилась идея найти булеву функцию F, которая при применении к «лапке» строила бы изображение «улыбки» и через все промежуточные изображения восстанавливала бы изображение «Чеширского кота». Такая функция была найдена, но для ее построения автору пришлось минимизировать булевы функции примерно 100 аргументов (ручным способом). Обобщив результаты по булевым преобразованиям двухградационных изображений, автор сформулировал и доказал теорему о существовании булевых функций, обеспечивающих произвольные заданные преобразования дискретных двухградационных изображений [1].

В 2001 г. при написании учебного пособия по булевой алгебре и комбинационным схемам [2] автор применил тот же метод для преобразования двоичных последовательностей. Двоичная последовательность B ($b_1, b_2, \ldots, b_n$) строится из двоичной последовательности A ($a_1, a_2, \ldots, a_n$) следующим образом. Каждый элемент b_i является результатом применения некоторой булевой функции F к элементу a_i и некоторым элементам из «окружения» a_i (слева и справа).

Пример 1. Пусть $A = 1011$. Возьмем в качестве F следующую функцию:

$$F = \neg a_{i-1} * a_i \vee \neg a_{i+2},$$

т. е. каждый элемент b_i последовательности B получается как конъюнкция инвертированного элемента, стоящего слева от a_i, и элемента a_i и дизъюнкции к полученному значению инвертированного элемента, стоящего справа через элемент от

a_i. Удобно такую функцию записать в виде: $F = \neg 1 * 0 \vee 2$. Результат применения такой функции к последовательности A дает последовательность $B = 1010$. Предполагается, что слева и справа от последовательности A стоят нули.

Теперь поставим задачу иначе. Пусть заданы две последовательности A и B одинаковой длины n. Нужно найти булеву функцию F, которая при применении к A строит B. В [2] обоснована процедура построения таблицы истинности такой функции. Первая строка содержит последовательность A, вторая — ту же последовательность A, сдвинутую влево на один разряд, третья — на два разряда и т. д. Всего в таблице истинности n строк. Каждой строке приписываются значения элементов последовательности B. Так, для рассмотренного выше примера получаем таблицу истинности:

−3	−2	−1	0	1	2	3	F
0	0	0	1	0	1	1	1
0	0	1	0	1	1	0	0
0	1	0	1	1	0	0	1
1	0	1	1	0	0	0	0

В качестве аргументов такой булевой функции берем элемент сдвинутый влево на 3 разряда (−3) от исходного (0), на 2 разряда влево (−2) и т. д. до элемента, сдвинутого от исходного на 3 разряда вправо (3). Всего для данного примера окажется 7 аргументов. В общем случае при длине последовательности n число аргументов равно $N = 2n - 1$. Функция N аргументов должна задаваться на 2^N наборах. Однако она задается всего на n наборах. На остальных наборах функция не определена. Число таких наборов равно $K = 2^N - n$. Следовательно, доопределить функцию можно 2^K способами. В примере при $n = 4$, $N = 7$ функция семи аргументов задавалась на четырех наборах, следовательно, на остальных $2^7 - 4 = 124$ наборах функция не определена и может быть доопределена 2^{124} способами. При грубой оценке $2^{10} > 10^3$ число способов доопределения функции превышает $16 * 10^{36}$. Следует заметить, что при любом способе доопределения последовательность $A = 1011$ функцией F будет преобразована в последовательность $B = 1010$. Из таблицы истинности легко увидеть, что функция $F = \neg 1$ также преобразует заданную последовательность A в B.

В [2] доказана теорема о существовании булевых функций, преобразующих заданное множество последовательностей A_i в множество последовательностей B_i, и определены требования, которым должны удовлетворять последовательности A_i (они не должны быть связаны сдвигом). Неоднозначность доопределения функции F, которую можно оценить величиной 2^K ($K = 2^N - n$, $N = 2n - 1$), исключительно быстро растет с ростом длины n, что позволило автору надеяться на возможное использование булевых преобразований при решении задач защиты информации от несанкционированного доступа.

Возможные применения

В настоящее время ведутся широкие исследования в области создания информационно-управляющих комплексов для сбора информации и управления автоматическими роботами-разведчиками (дистанционно пилотируемыми летательными аппаратами — ДПЛА) [3, 5]. Передача информации выполняется как по радиорелейным линиям, так и по локальным и глобальным сетям, включая Internet. В связи с этим важными проблемами становятся унификация и учет особенностей применения средств защиты информации от перехвата и незаконного использования в конкретных приложениях. Существующие симметричные и несимметричные криптографические системы позволяют решать часть задач защиты информации, однако при существенном увеличении числа управляемых объектов возникают сложности с присвоением проверяемых паролей, защитой сигналов управления от намеренного искажения. Так, в некоторых случаях «перехватчик» может осуществлять наблюдение за ДПЛА и пытаться сопоставить передаваемые команды управления и маневры аппарата. Для обеспечения непредсказуемости поведения ДПЛА в этих случаях целесообразно каждому сигналу управления сопоставлять большое число передаваемых команд, которые могут быть расшифрованы только средствами, находящимися в распоряжении ДПЛА.

Другой широкой областью применения средств защиты информации является использование Internet для управления разнообразной бытовой техникой [4]. Как и в предыдущем случае, возможны перехват и намеренное искажение как управляющих сигналов, так и сигналов состояния управляемых объектов.

В некоторой степени эти проблемы могут быть решены с помощью применения булевых преобразований передаваемых сигналов.

В работе [2] рассмотрена задача построения булевой функции F, которая преобразует любую двоичную n-разрядную последовательность A_i ($i = 1, 2, 3, \ldots, k$) множества последовательностей A в соответствующую последовательность B_i множества последовательностей B. Было показано, что если в множестве A нет последовательностей, связанных сдвигом, то такая функция всегда существует. Элементы последовательности B_i получались булевым преобразованием элементов последовательности A_i. В этой работе предлагается процедура, позволяющая находить такую функцию F, которая сводится к минимизации слабоопределенных булевых функций большого числа аргументов. В качестве примера использования этой односторонней функции приводится задача с избыточными паролями. Задача ставится следующим образом. Некоторое число пользователей (например, s) имеют по v паролей каждый и случайным образом подписывают свои сообщения одним из своих паролей. На приемном конце производится обработка всех подписей одной и той же функцией F, что позволяет идентифицировать пользователя. Перехватчик вводится в заблуждение тем, что сообщения подписываются различными паролями. Другим примером может служить задача управления объектами, в которой число команд, подлежащих шифрованию, может превышать несколько десятков миллионов. В связи с этим оказалось необходимо уточнить некоторые понятия и процедуры.

При преобразованиях множества двоичных комбинаций часто выбираются комбинации, не связанные сдвигом. Например, 10111001000 и 00101110010 —

последовательности, связанные сдвигом. Обе эти последовательности имеют одинаковый вес по Хэммингу $r = 5$ и совпадают при сдвиге второй последовательности на два разряда влево.

В общем случае две последовательности A_i (a_{i1}, a_{i2}, ..., a_{in}) и A_j (a_{j1}, a_{j2}, ..., a_{jn}) называют *связанными* сдвигом, если они имеют одинаковый вес по Хэммингу, т. е. $|A_i| = |A_j| = r$ и в функции взаимной корреляции имеют отсчет, равный r. Простая программная реализация позволяет из множества двоичных кодов длины n отобрать коды, не связанные сдвигом и использовать только их в качестве кодовых комбинаций, а именно,

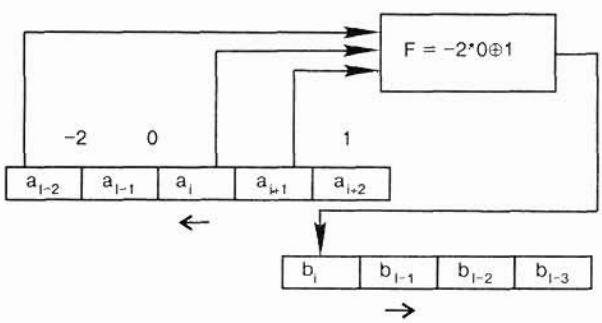
$$B(\tau) = \sum_{\tau=0}^{n-1} \sum_{k=1}^{n} a_{i,k}\, a_{j,k+\tau}\,.$$

Если при каком-то значении τ_0 $B(\tau_0) = r$, то последовательности A_i и A_j связаны сдвигом. Пусть при общей длине кода, равной n, число таких кодов равно $R(n)$. Тогда число кодов не связанных сдвигом, определяется разностью $2^n - R(n)$.

Для минимизации слабоопределенных булевых функций большого числа аргументов может быть использована процедура отбрасывания неинформативных аргументов, например, следующая. Исходное число аргументов в соответствии с процедурой, описанной в [2], равняется $2n - 1$. В таблице, построенной путем сдвига k исходных последовательностей A_i и приписывания им значений k последовательностей B_i, нет двух одинаковых строк. Следовательно, не может возникнуть ситуации, при которой одинаковым наборам аргументов должны соответствовать разные значения функции, т. е. на nk наборах функция была определена. Однако на остальных $N = 2^{2n-1} - nk$ наборах функция не определена, и ее можно доопределить 2^N способами. В результате минимизации нужно отобрать такие s аргументов, на которых наборы, где функция равна 1, отличались бы от наборов, на которых функция равна 0. Простой алгоритм перебора с отбрасыванием неинформативных аргументов позволяет проводить минимизацию при больших значениях n и k (в проведенных экспериментах до $n = k = 32$, однако, значения n и k могут быть легко увеличены без изменения процедуры минимизации).

Пример 2. Пусть заданы два множества последовательностей A и B:

$$A_1 = 101110010110110010110011 \rightarrow$$
$$\rightarrow B_1 = 100010111100100100011101,$$



■ ***Рис. 1.*** *Аппаратная реализация булевого преобразования двоичных последовательностей*

$$A_2 = 111010001101010100011101 \rightarrow$$
$$\rightarrow B_2 = 011110010100111001010101,$$
$$A_3 = 100111010001101111100100 \rightarrow$$
$$\rightarrow B_3 = 110001110111110010001001.$$

Легко видеть, что последовательности A_i не связаны сдвигом, поэтому существует булева функция F, которая из любой последовательности A_i строит соответствующую ей последовательность B_i. Вычисление этой функции оказалось достаточно простой задачей. Была разработана программа минимизации булевых слабоопределенных функций с числом аргументов 32. При необходимости число аргументов функции можно существенно увеличить. Функция имеет вид:

$$F = \neg{-1}*\neg 0*\neg 2 \vee -1*0*\neg 3 \vee -2*-1*3 \vee$$
$$\vee -1*0*\neg 1*4 \vee 1*\neg 2*3*4 \vee \neg{-1}*\neg 0*\neg 3 \vee$$
$$\vee \neg 0*\neg 1*2*6 \vee -3*-2*\neg{-1}*\neg 2 \vee \neg 0*\neg 2*\neg 3*5 \vee$$
$$\vee -1*0*\neg 1*\neg 3 \vee -1*\neg 0*\neg 1*2*3 \vee \neg{-1}*\neg 1*\neg 2*3 \vee$$
$$\vee -2*\neg{-1}*\neg 0*\neg 1*\neg 4 \vee -4*\neg{-1}*1*2 \vee \neg{-1}*\neg 0*4 \vee$$
$$\vee \neg{-2}*\neg 0*1*\neg 2 \vee 0*\neg 1*2*\neg 3*\neg 4 \vee \neg{-5}*\neg{-4}*0*\neg 2*3 \vee$$
$$\vee -2*0*1*\neg 2*3 \vee \neg 0*1*4 \vee 0*\neg 1*2*5 \vee$$
$$\vee \neg{-3}*-1*0*\neg 1 \vee 0*\neg 1*3*4, \qquad (1)$$

где 0 — элемент без сдвига, −1 — элемент со сдвигом влево на один разряд, −2 — на два разряда и т. д., 1 — элемент со сдвигом вправо на один разряд и т. п. Например, если A = 101101, F = $= \neg 0*2 \vee 1$. Требуется определить последовательность B. Первый разряд последовательности определяем как инверсию первого разряда последовательности A ($\neg 1 = 0$), логически умноженной на третий разряд (1) к результату логически прибавляем второй разряд (0), т. е. результат будет равен 0. Общий результат преобразования будет равен B = 011010.

Известно, что булевы операции выполняются исключительно быстро как аппаратными, так и программными средствами, поэтому реализация функции F двенадцати (и много большего числа) аргументов сложности не представляет.

Общая схема аппаратной реализации булевого преобразования показана на рис. 1.

На схеме для примера взята функция $F = -2*0 \oplus 1$.

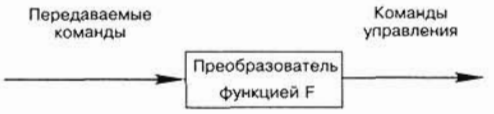
Для паролей нецелесообразно использовать сигналы с малым числом единиц или с малым числом нулей. Лучше всего, если число 1 и 0 будет примерно равно, в этом случае кодовая последовательность может оказаться близкой к случайной. Кроме того, выбираемые пароли не должны быть связаны сдвигом, чтобы могли обрабатываться одной булевой функцией F. Определим число таких сигналов для выбранной длины пароля n. В [2] найдено число кодов длины n веса q, не связанных сдвигом. Оно равно

$$S(n, q) = P(n - q, q - 1) = \overset{q-1}{\underset{n-1}{\mathbf{C}}}, \qquad (2)$$

где $P(a, b)$ — число перестановок из a объектов одного вида — единиц и b объектов другого — нулей.

При четном $n = 2k$ из соотношения (2) получим число кодов, вес которых равен половине их длины: $S(2k, k) = P(k, k - 1) = (2k - 1)!/k!(k - 1)!$.

■ ***Рис. 2.*** *Схема передачи изображений летательного аппарата на станцию обеспечения полета*



■ ***Рис. 3.*** *Схема скрытой передачи сигналов управления*

Подсчитаем число комбинаций длины $n = 2k$, не связанных сдвигом, если число единиц равно половине длины кода или отличается от половины на 1 (+ или −):

$$S(2k, k-1) + S(2k, k) + S(2k, k+1) =$$

$$= \underset{2k-1}{\overset{k-2}{\mathbf{C}}} + \underset{2k-1}{\overset{k-1}{\mathbf{C}}} + \underset{2k-1}{\overset{k}{\mathbf{C}}} =$$

$$= \underset{2k-1}{\overset{k-1}{\mathbf{C}}} (3k+1)/2k = \underset{n}{\overset{n/2-1}{\mathbf{C}}} (3n+2)/2n, \qquad (3)$$

где $S(2k, k-1)$ — число кодов, не связанных сдвигом, веса $k-1$; $S(2k, k)$ — число кодов, не связанных сдвигом, веса k; $S(2k, k+1)$ — число кодов, не связанных сдвигом, веса $k+1$, при этом все коды имеют длину $2k$.

Используя формулу Стирлинга: $n! = (2\pi n)^{1/2} n^n e^{-n}$ при $n \to \infty$, получим,что число комбинаций, не связанных сдвигом, веса 15,16 и 17 при $n = 32$ равно примерно $868*10^6$, т. е. составляет около 20 % от общего числа двоичных комбинаций длины $n = 32$ (которое равно примерно $4300*10^6$).

Рассмотрим несколько типовых задач шифрования информации при передаче по открытому каналу (допускающему возможность перехвата).

1. Передача изображений от дистанционно пилотируемого летательного аппарата на станцию обеспечения полета.

Схема такой передачи приведена на рис. 2.

Яркость точки преобразуется функцией F_1 таким образом, чтобы изображение было полностью искажено. На приемном конце производится восстановление истинной яркости с помощью функции F_2. Эта же задача может быть решена и с помощью других способов преобразования. Преимущество использования булевых функций состоит в том, что все кодовые комбинации преобразуются одной функцией, причем реализация преобразования производится в реальном масштабе времени (практически без задержки). Для преобразования кода яркости в коды, не связанные сдвигом, достаточно добавить 1 в старшем либо младшем разряде кода яркости. После чего с помощью функции F_1 можно преобразовать эти коды таким образом, чтобы изображение было полностью искажено. На приемном конце с помощью функции F_2 можно восстановить истинные яркости изображения.

Пример 3. Рассмотрим простой случай, когда число градаций яркости равно 8. Пусть яркости кодируются двоичными последовательностями от 000 до 111. Результат их преобразования функциями F_1 и F_2 приведен в табл. 1.

Функция F_1 имеет вид:

$$F_1 = -2*-1*\neg 1 \vee 0*1*2 \vee \neg -2*0*1 \vee$$
$$\vee -3*\neg -1*0 \vee 3 \vee \neg -1*2 \vee \neg -2*1*\neg 2 \vee \neg -2*\neg -1*0 \vee$$
$$\vee \neg -1*\neg 0*1 \vee \neg -3*\neg 0*\neg 1*\neg 2. \qquad (3)$$

Функция F_2 может быть представлена в виде:

$$F_2 = -3*\neg -2*0 \vee \neg -3*-2*\neg 0*\neg 1 \vee \neg -2*\neg -1*\neg 0 \vee$$
$$\vee \neg -3*\neg -1*\neg 0*\neg 1 \vee -1*\neg 0*1*\neg 2 \vee -3*\neg -1*0 \vee$$
$$\vee \neg 0*\neg 1*2 \vee -2*-1*1 \vee -1*0*2 \vee -1*\neg 1*2. \qquad (4)$$

В реальных системах число градаций яркости обычно равно 2^8, что может быть легко реализовано с помощью приведенной процедуры.

2. Скрытая передача сигналов управления на автономные объекты.

Схема такой передачи приведена на рис. 3.

Передаваемые команды выбираются так, чтобы после преобразования функцией F получить требуемые сигналы управления. Например, пусть имеется таблица соответствия передаваемых команд и команд управления (табл. 2).

Булева функция для такого преобразования имеет вид:

$$F = \neg 0*\neg 1*\neg 2 \vee -3*-1*\neg 1*\neg 2 \vee -1*2*3 \vee$$
$$\vee \neg 0*1*2*4 \vee \neg -4*-1*\neg 1*\neg 2*\neg 3 \vee \neg -3*-1*1*\neg 2*\neg 3 \vee$$

■ ***Таблица 1***

Исходные коды яркости	*Преобразование в коды, не связанные сдвигом*	*Результат преобразования функций F_1*	*Результат восстановления яркости функций F_2*
000	1000	1110	0000
001	1001	1011	0001
010	1010	1100	0010
011	1011	1000	0011
100	1100	1010	0100
101	1101	1001	0101
110	1110	1111	0110
111	1111	1101	0111

■ ***Таблица 2***

Команды, передаваемые по открытому каналу	*Команды управления оборудованием*
10100011	01110011
01111010	11010001
11101001	10110010
10010111	10101100
00111010	10111001
11001011	10110101
01001110	00100111
01111100	10100111

$$\vee -1*\rceil 0*3 \vee \lceil -2*-1*0*\rceil 1*\rceil 3 \vee -1*\rceil 0*1*2 \vee$$
$$\vee \rceil 0*\rceil 2*3 \vee -2*-1*\rceil 0*\rceil 1 \vee \lceil -2*\rceil -1*0*1*\rceil 2 \vee$$
$$\vee \lceil -3*-1*0*\rceil 1*2 \vee 1*\rceil 2*3*\rceil 6 \vee \lceil -1*0*\rceil 3*4 \vee$$
$$\vee \lceil -2*\rceil -1*\rceil 0*\rceil 1 \vee -2*\rceil -1*0*2 \vee \lceil -2*\rceil -1*\rceil 2*3*\rceil 4 \vee$$
$$\vee -2*\rceil -1*\rceil 0*\rceil 2 \vee -1*\rceil 0*1*4 \vee -2*0*1*3 \vee$$
$$\vee 0*1*2*3*\rceil 4 \vee 0*\rceil 1*\rceil 3*4 \vee \lceil -2*-1*\rceil 0*1. \quad (5)$$

Если перехватчик получит несколько пар передаваемых сигналов и соответствующих команд управления и попытается восстановить булеву функцию F, то он сформирует функцию, которая для других сигналов будет давать неверный результат. Так, в приведенном примере перехватчику могут быть известны пары:

10100011	01110011
01111010	11010001
11101001	10110010
10010111	10101100

По этим парам он вычислит булеву функцию, например, такую:

$$F* = \lceil -1*0*1 \vee -1*\rceil 0*1*2 \vee \lceil -1*1*\rceil 2 \vee$$
$$\vee \lceil -2*\rceil 1*\rceil 2*3 \vee \rceil 0*1*4 \vee \lceil -3*-1*0*\rceil 1*2 \vee$$
$$\vee \rceil 0*\rceil 1*\rceil 2 \vee -2*0*1 \vee \rceil 0*1*3 \vee \lceil -2*-1*0*\rceil 1 \vee$$
$$\vee \rceil 2*4 \vee \lceil -2*\rceil 0*\rceil 2.$$

Если применить эту булеву функцию к остальным четырем входным последовательностям, получим совершенно другие сигналы управления:

00111010	01101001
11001011	11010111
01001110	11011001
01111100	11011011

3. Передача сигналов управления и контроля на удаленные объекты.

Каждый тип удаленного объекта управления и контроля может снабжаться на входе собственной функцией F, вид которой зависит от типа объекта. Команда управления может быть общей для всех разнородных объектов, однако при обработке этой команды каждый тип объектов вырабатывает собственный сигнал управления. Схема передачи приведена на рис. 4.

Пусть сигналы управления для пяти типов объектов имеют вид: 1) 10010111; 2) 10111010; 3) 01110101; 4) 11001001; 5) 00111101.

Выберем некоторую общую команду, поступающую на все входы, например, такую: 11010111. Найдем для каждого устройства преобразующую функцию:

$$F_1 = \rceil 1*\rceil 2 \vee 0*1 \vee \lceil -1;$$
$$F_2 = 1*\rceil 2 \vee \rceil 0 \vee \lceil -1*\rceil 1;$$
$$F_3 = \rceil 1 \vee 0*2 \vee \rceil 0*\rceil 2;$$
$$F_4 = \rceil 1*\rceil 2 \vee \rceil 0*2 \vee -1*\rceil 1 \vee \lceil -1*\rceil 2;$$
$$F_5 = \rceil 1*\rceil 2 \vee 1*2 \vee \rceil 0 \vee \lceil -1*\rceil 1. \quad (6)$$

Легко убедиться в том, что из общей команды 11010111 с помощью соответствующей булевой функции F_1, F_2, F_3, F_4 или F_5 каждое устройство вырабатывает команду, предназначенную для данного типа устройства: 1, 2, 3, 4 или 5.

Если определить общее число разных команд, которые следует подавать на управляемые устройства и для каждого типа устройств определить необходимые команды управления, то легко вычислить булевы функции для каждого типа устройств. Снабдив на входе каждый тип устройств соответствующей булевой функцией, мы обеспечим как требуемое управление, так и скрытность передачи (даже перехватив несколько команд, достаточно трудно восстановить значение булевой функции).

4. Применение одноразовых ключей в системах связи объектов управления.

Управляющий центр и объект управления снабжаются одной булевой функцией F и набором исходных последовательностей $A_1, A_2, \ldots, A_k$.

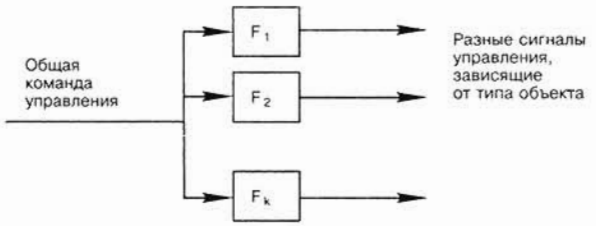
Из каждой исходной последовательности с помощью функции F центр и объект управления вырабатывают набор одноразовых ключей, например:

$$A_1 \to B_1 \to B_2 \to B_3 \to \ldots A_1,$$
$$A_2 \to C_1 \to C_2 \to C_3 \to \ldots A_2,$$
$$\ldots\ldots\ldots\ldots$$
$$A_k \to \ldots\ldots\ldots \to \ldots\ldots\ldots A_k,$$

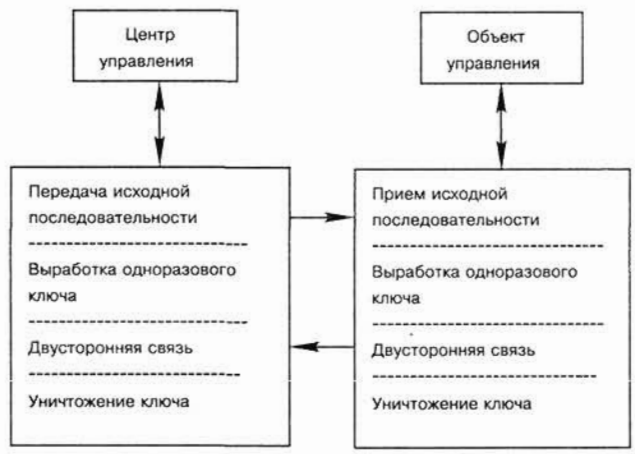
которые после каждого сеанса связи уничтожаются.

Схема связи приведена на рис. 5.

Пример 4. Пусть заданы последовательности: A_1 = 11010111; A_2 = 10010011; A_3 = 01110101; A_4 = 10100111.



■ ***Рис. 4.*** *Схема передачи сигналов управления*



■ ***Рис. 5.*** *Схема связи при использовании одноразовых ключей*

Определим булеву функцию, которая осуществляет следующее преобразование:

$$A_1 \to A_2 \to A_3 \to A_4 \to A_1.$$

$$F = -1*\neg 1*\neg 2 \vee -1*0*1 \vee \neg -2*0*2*\neg 4 \vee$$
$$\vee \neg 0*\neg 1*4 \vee \neg 0*\neg 3 \vee \neg -1*\neg 1*2 \vee \neg 1*\neg 2*\neg 3 \vee$$
$$\vee \neg -2*\neg -1*\neg 0 \vee \neg -2*\neg 2*4 \vee \neg -1*\neg 0*\neg 2 \vee 0*1*3. \quad (7)$$

Если функцию F представить не в дизъюнктивной нормальной форме, а в скобочной форме, получим более простое выражение:

$$F = \neg 0*(\neg 1*4 \vee \neg -1*(\neg -2 \vee \neg 2)) \vee$$
$$\vee \neg 2*(\neg 1*(-1 \vee \neg 3) \vee \neg -1*4) \vee$$
$$\vee 0*(1*(-1 \vee 3) \vee \neg -2*2*4) \vee \neg -1*\neg 1*2.$$

5. Ответы управляемых объектов с использованием различных паролей.

Центр передает сигналы запроса на объекты. Каждый объект для ответа использует несколько различных паролей (для маскировки). Центр обрабатывает ответы одной булевой функцией F и идентифицирует объект вне зависимости от выбранного им (из собственного списка) пароля.

Пример 5. Пусть имеется две группы объектов: X и Y.

Объект X используют следующие пароли:

101101
011011
100101.

Эти пароли при обработке функцией F центром должны дать код объекта X: 100011.

Объект Y пусть использует следующие пароли:

111011
001011
010111.

Эти пароли при обработке функцией F центром должны дать код объекта Y: 110111.

Функция $F = \neg 1*\neg 2 \vee -1*0*1 \vee 0*1*2 \vee 0*\neg 1*4 \vee \vee \neg -1*\neg 0*\neg 2 \vee 0*1*\neg 3 \vee \neg -2*1*\neg 3*4 \vee \neg -1*\neg 0*\neg 1 \vee \vee -3*1 \vee -1*\neg 2 \vee -1*1*2 \vee 5$ реализует эту процедуру.

6. Работа с большим числом объектов.

Число паролей может быть существенно увеличено без усложнения булевых функций, если использовать обратимые булевы преобразования, т. е. такие преобразования, при которых уравнение $F(X) = B$ при любых значениях вектора B имеет решение.

Важным вопросом является нахождение класса нетривиальных функций F, при которых уравнение $F(X) = B$ разрешимо относительно вектора $X(x_1, x_2, \ldots, x_n)$ при любых значениях элементов вектора $B(b_1, b_2, \ldots, b_n)$. Снабдив такой функцией F официального получателя сообщений, можно в центре управления по исходному тексту $B_1, B_2, B_3, \ldots$ вычислять криптотекст $X_1, X_2, X_3, \ldots$, который и передавать по открытому каналу. Официальный получатель, используя функцию F, восстановит исходное сообщение, так как $B_1 = F(X_1)$, $B_2 = F(X_2)$, $B_3 = F(X_3)$ и т. д. Кроме того, такой способ позволяет значительно увеличить число используемых паролей без существенного усложнения метода нахождения функций и паролей.

В качестве примера такой функции F для восьмиразрядных произвольных векторов $B(b_1, b_2, \ldots, b_8)$ можно взять функцию $F = \neg a_{i-1} \oplus a_0 \oplus a_{i+2}$. Значения элементов вектора X для этой функции определяются следующим образом:

$$\begin{aligned}
x_1 &= b_1 \oplus b_4 \oplus b_5 \oplus b_6 \oplus b_8 \oplus 1;\\
x_2 &= b_3 \oplus b_4 \oplus b_5 \oplus b_7;\\
x_3 &= b_4 \oplus b_5 \oplus b_6 \oplus b_8;\\
x_4 &= b_1 \oplus b_2 \oplus b_3 \oplus b_6 \oplus b_7 \oplus b_8;\\
x_5 &= b_6 \oplus b_7 \oplus b_8 \oplus 1;\\
x_6 &= b_1 \oplus b_2 \oplus b_3 \oplus b_5 \oplus b_7 \oplus 1;\\
x_7 &= b_1 \oplus b_2 \oplus b_3 \oplus b_5;\\
x_8 &= b_1 \oplus b_2 \oplus b_3 \oplus b_5 \oplus b_8 \oplus 1. \qquad (8)
\end{aligned}$$

Это можно записать в виде матричного произведения: $F^{-1} * B = X$.

Для примера выберем в качестве паролей все буквы латинского алфавита от A до Z. Сигналы запроса можно вычислить с помощью соотношения (9):

$$\begin{pmatrix} 100111011\\ 001110100\\ 000111010\\ 111001110\\ 000001111\\ 111010101\\ 111010000\\ 111010011 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 00000000000000000000000000\\ 11111111111111111111111111\\ 00000000000000000000000000\\ 00000000000000011111111111\\ 00000001111111100000000111\\ 00011110000111100001111000\\ 01100110011001100110011001\\ 10101010101010101010101010\\ 11111111111111111111111111 \end{pmatrix} =$$

$$= \begin{pmatrix} 01001010101101001011010101\\ 01100111100110011001100001\\ 10110101010010110100101010\\ 00101101001011010010110100\\ 00101101001011010010110100\\ 01100111100110000110011110\\ 11111110000000011111111000\\ 10101011010101001010101101 \end{pmatrix}. \qquad (9)$$

В выражении (9) первая матрица соответствует F^{-1}, вторая — B, результирующая — X. В матрице B в столбцах представлены коды всех букв от A до Z, последняя строка из единиц введена для того, чтобы учесть необходимые инверсии в преобразовании (8).

Например, передав полностью бессмысленную последовательность символов: 01111101100110111100010101111010 и обработав ее побайтно функцией $F =]-1 \oplus 0 \oplus 2$, получим коды букв осмысленного текста HELP:

01001000(H)01000101(E)01001100(L)01010000(P).

Легко проверить, что если взять любой код из матрицы X и обработать его функцией F, получим соответствующий код в матрице B.

Все передаваемое сообщение можно разбить на блоки длины $n = 8$ и шифровать каждый блок. Можно разбить на блоки другой длины, например, $n = 5$ или $n = 6$. В этом случае перехватчик, кроме подбора функции F, которая зависит от длины блока, должен еще подобрать длину блока n.

В рассмотренном случае не накладывается никаких ограничений на последовательности (они могут быть любыми и даже связанными сдвигом). Автору представляется реальной задача выбора некоторой функции F, например, для 32 разрядной последовательности, и нахождения уравнения, аналогичного (9). В этом случае число паролей будет превышать 4 миллиарда.

При необходимости можно брать последовательности значительно большей длины.

Следует заметить, что использование булевых преобразований во всех рассмотренных случаях не препятствуют применению средств защиты от помех, в частности, кодов, исправляющих как независимые ошибки в каналах связи, так и пакеты ошибок.

Заключение

В статье предложено использовать метод булевых преобразований двоичных последовательностей для решения различных задач контроля и управления подвижными объектами.

Показано, что нахождение булевых преобразований центром управления осуществляется достаточно просто, однако из-за неоднозначности доопределения получаемых слабоопределенных булевых функций криптоаналитику (незаконному перехватчику сообщений) даже при большом числе перехваченных пар сигналов практически невозможно восстановить функцию, выбранную центром управления.

Использование простых, быстровычислимых булевых функций может существенно расширить область применения средств защиты информации в случаях работы с большим количеством контролируемых и управляемых объектов.

Автор выражает искреннюю благодарность профессору Сергееву М. Б. за интерес, проявленный им к данной тематике, и настойчивость, благодаря которой была написана эта статья.

Литература

1. **Ерош И. Л., Игнатьев М. Б., Москалев Э. С.** Адаптивные робототехнические системы. /Учебное пособие для вузов. — Л., 1985. — 144 с.
2. **Ерош И. Л.** Дискретная математика. Булевы функции, комбинационные схемы, преобразования двоичных последовательностей: Учебное пособие. — СПб., 2001. — 38 с.
3. **Астапкович А. М., Анисимов А. Л., Елисеенко А. Г., Суханов И. О.** Современные тенденции построения систем управления дистанционно пилотируемыми летательными аппаратами. // В кн.: Информационно-управляющие системы для подвижных объектов. — СПб.: Политехника, 2002. — С. 7–32.
4. **Сергеев М. Б., Чудиновский Ю. Г.** IP-сеть как основа построения распределенных информационно-управляющих систем. // В кн.: Информационно-управляющие системы для подвижных объектов. — СПб.: Политехника, 2002. — С. 33–42.
5. **Анисимов А. Л., Астапкович А. М., Кравченко Д. А., Сергеев М. Б.** Контроль целостности радиоканала в системе дистанционного управления подвижными объектами. // В кн.: Информационно-управляющие системы для подвижных объектов. — СПб.: Политехника, 2002. — С. 100–109.
6. **Ерош И. Л.** Булевы преобразования в системах с открытым распределением ключей для задач управления подвижными объектами. // В кн.: Информационно-управляющие системы для подвижных объектов. — СПб.: Политехника, 2002. — С. 109–118.