собственных излучений компьютера), не уделяя должного внимания защите от несанкционированного доступа. Нельзя бросать все силы на защиту от атак из Интернет, не принимая мер по разграничению доступа к информации для своих сотрудников. Как бы лояльны и проверены не были ваши сотрудники, но исторический опыт показал, что самая конфиденциальная, жизненно важная информация иногда продается и за тридцать серебренников. И единственный путь уменьшить свои потери за счет утечки информации - это серьезное отношение к ее защите.

УДК 004.621

И.В.Васюков

СВЕДЕНИЕ НЕЛИНЕЙНОГО ВЗАИМНООДНОЗНАЧНОГО ПРЕОБРАЗОВАНИЯ В ПОЛЯХ ГАЛУА К СИСТЕМЕ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ РАНДОМИЗАЦИИ СООБЩЕНИЙ.

Одним из направлений повышения криптостойкости систем, использующих блочные шифры с предварительной рандомизацией входных сообщений, является введение нелинейности между этапами рандомизации и собственно криптографического преобразования [1]. В качестве нелинейности можно выбрать операцию обращения элементов, поскольку для любого элемента x конечного поля обратный элемент y существует по определению (за исключением лишь нулевого элемента). При этом следует понимать, что элемент y является обратным по отношению к x в смысле равенства единице произведения этих элементов.

$$x \cdot y = 1 \tag{1}$$

Тогда процедура нахождения элемента

$$y = \frac{1}{x}$$

может состоять в решении уравнения (1) при известном x. Для аналитического описания векторов данных в задачах криптографии обычно используются полиномы над полем Галуа $GF(2^n)$, коэффициенты которых совпадают с битовыми значениями соответствующих компонентов блока входных данных. Так двоичному вектору блока данных $\bar{x}$

$$\bar{x} = \{ x_{n-1}, \quad x_{n-2}, \quad \text{K}, \quad x_i, \quad \text{K}, \quad x_2, \quad x_1, \quad x_0 \}$$

в поле $GF(2^n)$ соответствует полином $X(z)$:

$$X(z) = x_{n-1}z^{n-1} \oplus x_{n-2}z^{n-2} \oplus \Lambda \oplus x_i z^i \oplus \Lambda \oplus x_2 z^2 \oplus x_1 z^1 \oplus x_0 z^0,$$

а двоичному вектору блока данных $\bar{y}$ соответствует полином $Y(z)$:

$$Y(z) = y_{n-1}z^{n-1} \oplus y_{n-2}z^{n-2} \oplus \Lambda \oplus y_i z^i \oplus \Lambda \oplus y_2 z^2 \oplus y_1 z^1 \oplus y_0 z^0.$$

Построение обратного элемента $Y(z)$ по известному элементу $X(z)$ можно выполнить, например, с помощью алгоритма Евклида для нахождения наибольшего общего делителя [2] или с помощью метода индексного обращения [3].

Следует отметить, что использование алгоритма Евклида предполагает необходимость выполнения последовательности операций деления с остатком над полиномами, т.е. в плане вычислительной сложности этот алгоритм не проще операции деления полиномов, которая в явном виде присутствует в операции их обращения:

$$Y(z) = \frac{1}{X(z)}. \tag{2}$$

Использование метода индексного обращения основано на учете конечности поля

$GF(2^n)$. Количество элементов поля равно некоторой величине N. Поэтому каждой паре элементов $X(z)$ и $Y(z)$ можно поставить в соответствие индексы i и j таким образом, чтобы всегда выполнялось условие $i+j=N$. Тогда зная индекс элемента $X_i(z)$ можно легко найти индекс элемента, обратного к нему по следующей формуле

$$j=N-i,$$

а по известному индексу j восстановить обратный элемент $Y_j(z)$. Метод индексного обращения удобен при относительно небольших значениях N, когда размеры таблиц значений элементов поля являются приемлемыми для их хранения в памяти спецпроцессоров. В общем же случае, когда N может быть $N=2^n$, а значения n для реальных величин блоков данных составляют в настоящее время 64 и 128 бит, количество значений, необходимых для хранения в памяти оцениваются величиной $N=2^{64}$ или даже $N=2^{128}$, что не реализуемо на современном этапе развития технологии средств компьютерной техники.

Таким образом, для использования нелинейного взаимнооднозначного преобразования в качестве способа повышения стойкости рандомизированных криптосистем с блочными шифрами необходимо обеспечить возможность решения задачи обращения элементов в полях Галуа таким образом, чтобы эта возможность допускала реализацию средствами вычислительной техники более простую, чем алгоритм Евклида или метод индексного обращения при значениях N, реально используемых в настоящее время.

Для реализации такой возможности перейдем от явной формы задания нелинейности в виде выражения (2) к неявной форме

$$X(z)\cdot Y(z)=1. \qquad (3)$$

Данная форма может рассматриваться в качестве полиномиального уравнения относительно $Y(z)$ при известном $X(z)$. Решение этого уравнения можно выполнить, например, методом неопределенных коэффициентов [4], который предполагает переход от одного полиномиального уравнения с n неизвестными коэффициентами полинома $Y(z)$ к системе n алгебраических уравнений относительно n неизвестных коэффициентов y_i полинома $Y(z)$.

Однако непосредственное применение метода неопределенных коэффициентов к уравнению (3) невозможно по следующей причине. Каждый из полиномов $X(z)$ и $Y(z)$ в общем случае содержит n членов и степень каждого из полиномов в общем случае равна $(n-1)$. Многочлен, являющийся произведением полиномов $X(z)$ и $Y(z)$, будет содержать $(2n-1)$ членов и иметь степень $(2n-2)$. Поэтому система алгебраических уравнений, к которой приводится полиномиальное уравнение (3), будет содержать $(2n-1)$ уравнений. Однако количество неизвестных коэффициентов y_i полинома $Y(z)$ по-прежнему остается равным n. Таким образом, система уравнений, формируемая на основании уравнения (3), оказывается переопределенной. Попытки решить эту систему отбрасыванием каких-либо $(n-1)$ из ее уравнений, или использованием метода наименьших квадратов [5], не приводят к результату, обеспечивающему точное выполнение соотношения (3).

Известно [6], что если полиномы $X(z)$ и $Y(z)$ являются полиномами над полем $GF(2^n)$, и структура поля задана неприводимым полиномом $m(z)$ степени не выше чем $(n-1)$, то все элементы этого поля также имеют степень не выше чем $(n-1)$. Следовательно, и произведение полиномов $X(z)$ и $Y(z)$ в поле $GF(2^n)$ тоже должно иметь степень не выше, чем $(n-1)$.

В скобках отметим, что в дальнейшем поле $GF(2^n)$, структура которого задается

неприводимым полиномом $m(z)$, в будем обозначать $GF(2^n)/m(z)$.

Кроме того, известно, что все степени переменной z, которые превышают $(n-1)$, имеют в поле $GF(2^n)/m(z)$ тождественные представления в виде полиномов, степень которых не выше $(n-1)$. Например, если при $n=8$ структура поля $GF(2^8)$ задана неприводимым полиномом

$$m(z) = z^8 \oplus z^4 \oplus z^3 \oplus z \oplus 1, \qquad (4)$$

то таблица степеней z выглядит так, как это показано в таблице 1.

Таблица 1.

Степень	Результат	Степень	Результат
z^0	1	z^{26}	$z^1+z^3+z^4+z^5+z^6+z^7$
z^1	z^1	z^{27}	$1+z^1+z^2+z^3+z^5+z^6+z^7$
z^2	z^2	z^{28}	$1+z^2+z^6+z^7$
z^3	z^3	z^{29}	$1+z^4+z^7$
z^4	z^4	z^{30}	$1+z^3+z^4+z^5$
z^5	z^5	z^{31}	$z^1+z^4+z^5+z^6$
z^6	z^6	z^{32}	$z^2+z^5+z^6+z^7$
z^7	z^7	z^{33}	$1+z^1+z^4+z^6+z^7$
z^8	$1+z^1+z^3+z^4$	z^{34}	$1+z^2+z^3+z^4+z^5+z^7$
z^9	$z^1+z^2+z^4+z^5$	z^{35}	$1+z^5+z^6$
z^{10}	$z^2+z^3+z^5+z^6$	z^{36}	$z^1+z^6+z^7$
z^{11}	$z^3+z^4+z^6+z^7$	z^{37}	$1+z^1+z^2+z^3+z^4+z^7$
z^{12}	$1+z^1+z^3+z^5+z^7$	z^{38}	$1+z^2+z^5$
z^{13}	$1+z^2+z^3+z^6$	z^{39}	$z^1+z^3+z^6$
z^{14}	$z^1+z^3+z^4+z^7$	z^{40}	$z^2+z^4+z^7$
z^{15}	$1+z^1+z^2+z^3+z^5$	z^{41}	$1+z^1+z^4+z^5$
z^{16}	$z^1+z^2+z^3+z^4+z^6$	z^{42}	$z^1+z^2+z^5+z^6$
z^{17}	$z^2+z^3+z^4+z^5+z^7$	z^{43}	$z^2+z^3+z^6+z^7$
z^{18}	$1+z^1+z^5+z^6$	z^{44}	$1+z^1+z^7$
z^{19}	$z^1+z^2+z^6+z^7$	z^{45}	$1+z^2+z^3+z^4$
z^{20}	$1+z^1+z^2+z^4+z^7$	z^{46}	$z^1+z^3+z^4+z^5$
z^{21}	$1+z^2+z^4+z^5$	z^{47}	$z^2+z^4+z^5+z^6$
z^{22}	$z^1+z^3+z^5+z^6$	z^{48}	$z^3+z^5+z^6+z^7$
z^{23}	$z^2+z^4+z^6+z^7$	z^{49}	$1+z^1+z^3+z^6+z^7$
z^{24}	$1+z^1+z^4+z^5+z^7$	z^{50}	$1+z^2+z^3+z^7$
z^{25}	$1+z^2+z^3+z^4+z^5+z^6$	z^{51}	1

Используя тождественные полиномы для замены в произведении $X(z)$ и $Y(z)$ всех

степеней z, которые превышают $(n-1)$, можно перейти от уравнения (3) к уравнению

$$P_{x,y}(z)=1, \tag{5}$$

где $P_{x,y}(z)$ есть полином, степени не выше чем $(n-1)$, и каждый из коэффициентов многочлена $P_{x,y}(z)$ зависит в общем случае от всех коэффициентов полиномов $X(z)$ и $Y(z)$, т.е. зависит от всех компонентов векторов $\bar{x}$ и $\bar{y}$:

$$P_{x,y}(z)=p_{n-1}(\bar{x},\bar{y})\cdot z^{n-1}\oplus p_{n-2}(\bar{x},\bar{y})z^{n-2}\oplus\Lambda\oplus p_1(\bar{x},\bar{y})z^1\oplus p_0(\bar{x},\bar{y})z^0. \tag{5}$$

Представим единицу в правой части уравнения (5) в виде полинома по z следующим образом

$$1=0\cdot z^{n-1}\oplus 0\cdot z^{n-2}\oplus\Lambda\oplus 0\cdot z^{i}\oplus\Lambda\oplus 0\cdot z^{2}\oplus 0\cdot z^{1}\oplus 1\cdot z^{0} \tag{6}$$

и приравняем коэффициенты при одинаковых степенях z в правых частях выражений (5) и (6). Получим систему из n уравнений

$$\begin{cases} p_{n-1}(\bar{x},\bar{y})=0, \\ p_{n-2}(\bar{x},\bar{y})=0, \\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda \\ p_2(\bar{x},\bar{y})=0, \\ p_1(\bar{x},\bar{y})=0, \\ p_0(\bar{x},\bar{y})=1. \end{cases} \tag{6}$$

относительно n неизвестных битовых элементов вектора $\bar{y}$:

$$\bar{y}=\{\,y_{n-1},\ \ y_{n-2},\ \ \mathrm{K},\ \ y_i,\ \ \mathrm{K},\ \ y_2,\ \ y_1,\ \ y_0\,\}$$

Коэффициентами при неизвестных значениях y_i в системе уравнений (6) также выступают битовые значения, сформированные из сумм по модулю 2 соответствующих битовых компонентов вектора $\bar{x}$. При каждом конкретном значении блока входных данных битовые компоненты вектора $\bar{x}$ принимают конкретные значения и система уравнений (6) становится системой линейных алгебраических уравнений с постоянными битовыми коэффициентами. В общем виде такую систему уравнений можно записать следующим образом:

$$\mathbf{B}_{\bar{x}}\cdot\bar{y}=\bar{1}, \tag{7}$$

где $\mathbf{B}_{\bar{x}}$ - матрица, элементами которой являются битовые значения 0 или 1, сформированные как результат суммы по модулю 2 битовых значений компонентов блока входных значений – вектора $\bar{x}$; $\bar{1}$ - единичный вектор, содержащий n компонентов и имеющий следующий вид:

$$\bar{1}=\{\,1,\ \ 0,\ \ 0,\ \ \mathrm{K},\ \ 0,\ \ \mathrm{K},\ \ 0,\ \ 0\,\}.$$

Можно показать, что для матрицы $\mathbf{B}_{\bar{x}}$ выполняется следующее соотношение:

$$\mathbf{B}_{\bar{x}}=\left[\sum_{i=0}^{n-1}\mathbf{B}_i x_i\right|_{\mathrm{mod}\,2}\Bigg], \tag{8}$$

где $\mathbf{B}_i$ $(i=0,\mathrm{K},n-1.)$ - матрицы, компонентами которых являются битовые

постоянные (0 или 1). Матрицы $\mathbf{B}_i$ являются постоянными для каждого конкретного поля $GF(2^n)/m(z)$. Примеры матриц $\mathbf{B}_i$ для поля $GF(2^8)/m(z)$ структура которого задана многочленом $m(z) = z^8 \oplus z^4 \oplus z^3 \oplus z \oplus 1$, представлены в виде выражений (8):

$$\mathbf{B}_0 = \begin{bmatrix} & & & & & & & 1 \\ & & & & & & 1 & \\ & & & & & 1 & & \\ & & & & 1 & & & \\ & & & 1 & & & & \\ & & 1 & & & & & \\ & 1 & & & & & & \\ 1 & & & & & & & \end{bmatrix}, \quad \mathbf{B}_1 = \begin{bmatrix} 1 & & & & & & & \\ 1 & & & & & & & 1 \\ & & & & & & 1 & \\ 1 & & & & & 1 & & \\ 1 & & & & 1 & & & \\ & & & 1 & & & & \\ & & 1 & & & & & \\ & 1 & & & & & & \end{bmatrix},$$

$$\mathbf{B}_2 = \begin{bmatrix} & 1 & & & & & & \\ 1 & 1 & & & & & & \\ 1 & & & & & & & 1 \\ & 1 & & & & & 1 & \\ 1 & 1 & & & & 1 & & \\ 1 & & & & 1 & & & \\ & & & 1 & & & & \\ & & 1 & & & & & \end{bmatrix}, \quad \mathbf{B}_3 = \begin{bmatrix} & & 1 & & & & & \\ & 1 & 1 & & & & & \\ 1 & 1 & & & & & & \\ 1 & & 1 & & & & & 1 \\ & 1 & 1 & & & & 1 & \\ 1 & 1 & & & & 1 & & \\ 1 & & & & 1 & & & \\ & & & 1 & & & & \end{bmatrix}, \quad (9)$$

$$\mathbf{B}_4 = \begin{bmatrix} & & & 1 & & & & \\ & & 1 & 1 & & & & \\ & 1 & 1 & & & & & \\ 1 & 1 & & 1 & & & & \\ 1 & & 1 & 1 & & & & 1 \\ & 1 & 1 & & & & 1 & \\ 1 & 1 & & & & 1 & & \\ 1 & & & & 1 & & & \end{bmatrix}, \quad \mathbf{B}_5 = \begin{bmatrix} 1 & & & & 1 & & & \\ 1 & & & 1 & 1 & & & \\ & & 1 & 1 & & & & \\ 1 & 1 & 1 & & 1 & & & \\ & 1 & & 1 & 1 & & & \\ 1 & & 1 & 1 & & & & 1 \\ & 1 & 1 & & & & 1 & \\ 1 & 1 & & & & 1 & & \end{bmatrix},$$

$$\mathbf{B}_6 = \begin{bmatrix} 1 & 1 & & & & 1 & & \\ & 1 & & & 1 & 1 & & \\ 1 & & & 1 & 1 & & & \\ 1 & 1 & 1 & 1 & & 1 & & \\ & & 1 & & 1 & 1 & & \\ & 1 & & 1 & 1 & & & \\ 1 & & 1 & 1 & & & & 1 \\ & 1 & 1 & & & & 1 & \end{bmatrix}, \qquad \mathbf{B}_7 = \begin{bmatrix} & 1 & 1 & & & & 1 & \\ 1 & & 1 & & & 1 & 1 & \\ & 1 & & & 1 & 1 & & \\ 1 & 1 & 1 & 1 & 1 & & 1 & \\ 1 & & & 1 & & 1 & 1 & \\ & & 1 & & 1 & 1 & & \\ & 1 & & 1 & 1 & & & \\ 1 & & 1 & 1 & & & & 1 \end{bmatrix},$$

В общем виде новая постановка задачи состоит в решении системы уравнений

$$\left[\sum_{i=0}^{n-1} \mathbf{B}_i x_i \Big|_{\mathrm{mod}\,2} \right] \cdot \bar{y} = \bar{1}, \tag{10}$$

при известных составляющих $\mathbf{B}_i$ и известных компонентах x_i вектора входных значений $\bar{x}$.

При этом возникает вопрос, каким методом решать систему уравнений (10), чтобы, во-первых, решение было точным, во-вторых, в процессе решения не возникало операций деления чисел (ограничение, обусловленное существованием алгоритма Евклида) и, в-третьих, вычислительная сложность такого решения оказалась меньше, чем 2^n операций (ограничение, обусловленное существованием алгоритма индексного обращения).

Наиболее известным из точных методов решения систем линейных алгебраических уравнений является метод Гаусса [7]. Напомним некоторые положения, которые потребуются в наших последующих рассуждениях. Прежде всего, отметим, что в методе Гаусса рассматривается система уравнений

$$\mathbf{A} \cdot \bar{y} = \bar{c}. \tag{11}$$

Здесь $\mathbf{A} = \lfloor a_{i,j} \rfloor$ - квадратная матрица размерности $n \cdot n$. В общем случае, метод Гаусса предполагает деление первого уравнения

$$\sum_{j=0}^{n-1} a_{0,j} \cdot y_j = c_0$$

системы (11) на коэффициент $a_{0,0}$ $(a_{0,0} \neq 0)$, в результате чего получается уравнение

$$y_0 + \sum_{j=1}^{n-1} a_{0,j}^{(1)} \cdot y_j = c_0^{(1)} \tag{12}$$

где $a_{0,j}^{(1)} = a_{0,j} / a_{0,0}$, $c_0^{(1)} = c_0 / a_{0,0}$. Затем уравнение (12) умножается на коэффициент $a_{i,0}$ (i=1, 2, 3, …, n-1) и вычитается из каждого i-го (i=1, 2, 3, …, n-1) уравнения системы (11), кроме первого (i=0). В результате приходим к системе уравнений

$$\mathbf{A}^{(1)} \cdot \bar{y} = \bar{c}^{(1)}, \tag{13}$$

в которой первое неизвестное y_0 оказывается исключенным из всех уравнений, кроме первого, а коэффициент при неизвестном y_0 в первом уравнении равен 1. Далее в

предположении, что $a_{1,1}^{(1)} \neq 0$, необходимо разделить второе уравнение системы (13) на коэффициент $a_{1,1}^{(1)}$ и исключить неизвестное y_1 из всех уравнений, начиная с третьего, и т.д. В результате последовательного исключения неизвестных система уравнений (11) с квадратной матрицей преобразуется в систему уравнений

$$y_i + \sum_{j=i+1}^{n-1} a_{i,j}^{(i+1)} \cdot y_j = c_i^{(i+1)}, \quad (i = 0,1,2,\ldots,\text{n-1}) \tag{14}$$

с треугольной матрицей. Последнее уравнение такой системы имеет вид

$$y_{n-1} = c_{n-1}^{(n)} \tag{15}$$

Совокупность преобразований, в ходе которых исходная задача приводится к системе уравнений вида (14), называется, как известно [6], прямым ходом метода Гаусса.

Последнее уравнение (15) системы (14) дает в явном виде значение y_{n-1}, которое подставляется в предпоследнее уравнение, в результате чего в явном виде определяется значение y_{n-2}, и т.д вплоть до получения в явном виде значения y_0. Совокупность преобразований, которые определяют значения неизвестных y_i в явном виде на основании уравнений (14) называется обратным ходом метода Гаусса.

В нашем случае исходная квадратная матрица имеет вид (8), т.е.

$$\mathbf{A} = \mathbf{B}_{\bar{x}} = \left[\sum_{i=0}^{n-1} \mathbf{B}_i x_i \Big|_{\mathrm{mod}\,2} \right].$$

Т.к. все компоненты составляющих матриц $\mathbf{B}_i$ являются битовыми элементами и при любых значениях x_i их сумма по модулю 2 также будет битовым элементом, то коэффициент при каждом неизвестном изначально равен либо нулю либо единице. Поэтому исчезает необходимость выполнять операцию деления уравнений системы на коэффициент при соответствующем неизвестном в прямом ходе метода Гаусса. Тем самым автоматически выполняется требование исключения операций деления. Необходимо лишь обеспечить преобразование квадратной матрицы $\mathbf{B}_{\bar{x}}$ в треугольную $\mathbf{B}_{\bar{x}}^{(n-1)}$. По аналогии с классическим методом Гаусса это достигается сложением по модулю 2 первой строки исходной матрицы $\mathbf{B}_{\bar{x}}^{(0)} = \mathbf{B}_{\bar{x}}$ со всеми остальными ее строками содержащими единицу в первом столбце. В результате выполнения первого шага формируется матрица $\mathbf{B}_{\bar{x}}^{(1)}$, первый столбец которой имеет вид

$$(1,\ 0,\ 0,\ \mathrm{K},\ 0,\ 0)^{\mathrm{T}}.$$

На втором шаге вторая строка матрицы $\mathbf{B}_{\bar{x}}^{(1)}$ складывается со всеми последующими строками матрицы $\mathbf{B}_{\bar{x}}^{(1)}$, содержащими единицу во втором столбце. В результате формируется матрица $\mathbf{B}_{\bar{x}}^{(2)}$, второй столбец которой имеет вид

$$(*,\ 1,\ 0,\ \mathrm{K},\ 0,\ 0)^{\mathrm{T}},$$

где знак (*) обозначает либо ноль, либо единицу. По аналогии, на третьем шаге получаем матрицу $\mathbf{B}_{\bar{x}}^{(2)}$ третий столбец которой имеет вид

$$(*,\ *,\ 1,\ \mathrm{K},\ 0,\ 0)^{\mathrm{T}}$$

и так далее. В итоге, после $(n-1)$ шагов прямого хода мы получим треугольную матрицу $\mathbf{B}_{\bar{x}}^{(n-1)}$. Отметим, что параллельно с преобразованием матрицы $\mathbf{B}_{\bar{x}}$ соответствующие опе́рации сложения по модулю 2 необходимо выполнять над компонентами вектора $\bar{1}$, представляющего правую часть системы уравнений (10).

Проиллюстрируем сказанное на примере. Пусть $n=8$ и вектор $\bar{x}$ задан в следующем виде:

$$\bar{x}=(0,\ \ 1,\ \ 0,\ \ 0,\ \ 0,\ \ 1,\ \ 1,\ \ 1),$$

т.е. $x_7=0,\ x_6=1,\ x_5=0,\ x_4=0,\ x_3=0,\ x_2=1,\ x_1=1,\ x_0=1$. Подставляя эти значения в выражение (10) получим:

$$\left[\mathbf{B}_6 \oplus \mathbf{B}_2 \oplus \mathbf{B}_1 \oplus \mathbf{B}_0\right]\cdot \bar{y}=\bar{1}. \qquad (16)$$

Подставляя в это выражение значения матриц $\mathbf{B}_i$ согласно (9) получим,

$$\begin{bmatrix} & & & & & 1 & & 1 \\ & & & & 1 & 1 & 1 & 1 \\ & & & 1 & 1 & 1 & 1 & 1 \\ & & 1 & 1 & 1 & & 1 & \\ & 1 & 1 & 1 & & & & \\ 1 & 1 & 1 & & & & & \\ 1 & 1 & & & & & & 1 \\ 1 & & & & & & 1 & \end{bmatrix} \cdot \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Для удобства дальнейших вычислений перегруппируем полученную систему уравнений в обратном порядке

$$\begin{bmatrix} 1 & & & & & & 1 & \\ 1 & 1 & & & & & & 1 \\ 1 & 1 & 1 & & & & & \\ & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 1 & & 1 & \\ & & & 1 & 1 & 1 & 1 & 1 \\ & & & & 1 & 1 & 1 & 1 \\ & & & & & 1 & & 1 \end{bmatrix} \cdot \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Сложим по модулю 2 первое уравнение этой системы со вторым и третьим уравнением. Получим

$$\begin{bmatrix} 1 & & & & & & 1 & \\ & 1 & & & & & 1 & 1 \\ & 1 & 1 & & & & 1 & \\ & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 1 & & 1 & \\ & & & 1 & 1 & 1 & 1 & 1 \\ & & & & 1 & 1 & 1 & 1 \\ & & & & & 1 & & 1 \end{bmatrix} \cdot \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

На втором шаге сложим второе уравнение полученной системы с третьим и четвертым. Получим

$$\begin{bmatrix} 1 & & & & & & 1 & \\ & 1 & & & & & 1 & 1 \\ & & 1 & & & & & 1 \\ & & 1 & 1 & & & 1 & 1 \\ & & 1 & 1 & 1 & & 1 & \\ & & & 1 & 1 & 1 & 1 & 1 \\ & & & & 1 & 1 & 1 & 1 \\ & & & & & 1 & & 1 \end{bmatrix} \cdot \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

На третьем шаге складываем третье уравнение с четвертым и пятым:

$$\begin{bmatrix} 1 & & & & & & 1 & \\ & 1 & & & & & 1 & 1 \\ & & 1 & & & & & 1 \\ & & & 1 & & & 1 & \\ & & & 1 & 1 & & 1 & 1 \\ & & & 1 & 1 & 1 & 1 & 1 \\ & & & & 1 & 1 & 1 & 1 \\ & & & & & 1 & & 1 \end{bmatrix} \cdot \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Далее, четвертое уравнение прибавляем по модулю 2 к пятому и шестому уравнениям. В результате выполнения четвертого шага получаем следующий результат:

$$\begin{bmatrix} 1 & & & & & & 1 & \\ & 1 & & & & & 1 & 1 \\ & & 1 & & & & & 1 \\ & & & 1 & & & 1 & \\ & & & & 1 & & & 1 \\ & & & & 1 & 1 & & 1 \\ & & & & 1 & 1 & 1 & 1 \\ & & & & & 1 & & 1 \end{bmatrix} \cdot \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Затем пятое уравнение складывается с шестым и седьмым:

$$\begin{bmatrix} 1 & & & & & & 1 & \\ & 1 & & & & & 1 & 1 \\ & & 1 & & & & & 1 \\ & & & 1 & & & 1 & \\ & & & & 1 & & & 1 \\ & & & & & 1 & & \\ & & & & & 1 & 1 & \\ & & & & & 1 & & 1 \end{bmatrix} \cdot \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

После чего шестое уравнение прибавляется к седьмому и восьмому.

$$\begin{bmatrix} 1 & & & & & & 1 & \\ & 1 & & & & & 1 & 1 \\ & & 1 & & & & & 1 \\ & & & 1 & & & 1 & \\ & & & & 1 & & & 1 \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{bmatrix} \cdot \begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

В результате мы получаем систему, решение которой очевидным образом формируется в процессе обратного хода:

$$y_0 = 1; \quad y_1 = 0; \quad y_2 = 0; \quad y_3 = 0 \oplus y_0 = 1; \quad y_4 = 0 \oplus y_2 = 0;$$
$$y_5 = 0 \oplus y_0 = 1; \quad y_6 = 0 \oplus y_1 \oplus y_0 = 1; \quad y_7 = 0 \oplus y_1 = 0.$$

Нетрудно проверить, что для реализации прямого хода метода Гаусса при решении систем уравнений в полях Галуа требуется порядка $n^3/3$ операций сложения модулю 2 одноразрядных булевых операндов. Реализация обратного хода требует не более $n^2/2$ таких же операций. Таким образом, общая оценка затрат составляет порядка $n^3/3 + n^2/2$ элементарных операций. Эта оценка ниже величины 2^n начиная с $n = 8$ и выигрыш тем больше, чем больше n. Например, при $n = 64$ кратность выигрыша по отношению к методу

индексного обращения составит величину порядка $10^{19}/10^{5}=10^{14}$.

Таким образом, переход от явной формы задания нелинейного преобразования к неявной и дальнейшее сведение неявной формы к системе линейных алгебраических уравнений с переменными коэффициентами в поле Галуа с последующим решением этой системы методом Гаусса позволяет существенно упростить вычислительную сложность задачи, открывая, тем самым, путь к использованию нелинейного взаимнооднозначного преобразования в полях Галуа в системах защиты информации, использующих, в частности, рандомизацию сообщений.

Список литературы:

1. Алексейчук А.Н., Васюков И.Н., Корнейко А.В. Метод построения и теоретико-информационный анализ стойкости рандомизированных криптосистем с секретным ключом. // Збірник наукових праць ІПМЕ НАН України. – 2003. - Вип.22. – С. 65-73

2. Андерсон Д.А. Дискретная математика и комбинаторика: Пер.с англ. – М.: Издательский дом «Вильямс», 2003. – 960 с.

3. Касперски К. Полиномиальная арифметика и поля Галуа или информация воскресшая из пепла // «Системный администратор». – 2003, № 10. – С. 84-90.

4. Фильчаков П.Ф. Справочник по высшей математике.- К.: «Наукова думка», 1972. – 743 с.

5. Лоусон Ч., Хенсон Р. Численное решение задач метода наименьших квадратов: Пер.с англ. – М.: «Наука», 1986. – 232 с.

6. Шнайер Б. Прикладная криптография. – М.: Изд-во ТРИУМФ, 2002. – 816 с.

7. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы. – М.: «Наука», 1987. – 600 с.

УДК 004.68

С.Р.Коженевский

УТЕЧКА ИНФОРМАЦИИ ЧЕРЕЗ НАКОПИТЕЛЬ НА ЖЕСТКОМ МАГНИТНОМ ДИСКЕ

За последние несколько десятилетий компьютерные информационные технологии прочно вошли в нашу жизнь и стали составной частью документооборота. Первоначально отработанные механизмы обеспечения информационной безопасности для новых компьютерных систем уже не подходят и требуют существенной модернизации. В первую очередь это относится к информации, хранящейся на жестком магнитном диске (НЖМД).

Ранее для снятия информации с НЖМД был необходим физический доступ к носителю. Появление же компьютерных сетей создало новые угрозы безопасности информации, так как позволяет дистанционно, а иногда и скрыто от пользователя, получить доступ к хранимой на компьютере информации.

В настоящее время на развитие индустрии защиты информации (ЗИ), тратятся миллионы долларов. А, по сути дела, решается одна задача - сделать открытую информацию доступной всем пользователям, а конфиденциальную - доступной только тому, кому она предназначается. Как в сфере бизнеса, так и в сфере государственного управления, уже скопились значительные объемы конфиденциальной информации, хранящиеся в базах данных персональных компьютеров (ПК). Эта информация представляет собой реальную ценность, а утечка ее в ряде случаев способна влиять даже на государственную безопасность.

Данное обстоятельство дало мощный толчок к развитию всевозможных программных и аппаратных средств добывания информации из ПК и компьютерных сетей. Особенно уязвимыми оказались сети, имеющие прямой выход в Интернет.

Пути или каналы утечки информации, позволяющие несанкционированно и