УДК 004.056.55

А.В. Корнейко, г. Киев

ОБОБЩЕННАЯ МОДЕЛЬ ПРЕОБРАЗОВАНИЙ В ПОЛЯХ ГАЛУА НЕЛИНЕЙНОГО РАНДОМИЗАТОРА ДЛЯ СИММЕТРИЧНЫХ БЛОЧНЫХ ШИФРОВ

Annotation. A generalized model of nonlinear randomizer for cryptographic information protection schemes that use symmetric block ciphers, which is a sequential operation of linear and nonlinear changes in the open message Galois fields, performed before the procedure block encryption.

Введение

Детальное обоснование использования различных методов рандомизации для повышения криптостойкости симметричных блочных шифров (СБШ), исследования стойкости таких рандомизированных криптосхем относительно основных типов криптоанализа достаточно полно проведено в ряде работ под руководством известного украинского ученого-криптографа А. Алексейчука, среди которых, например [1-3] и многие другие.

Эти исследования показали, что в отдельных случаях (например, при использовании группирования открытых сообщений при криптоанализе) линейная рандомизация не только не позволяет исключить криптографическую слабость («лазейку»), которая может быть случайно или целенаправлено заложена в конструкцию СБШ, но и даже усиливает ее эффект. Поэтому в [2] было предложено стойкость систем защиты информации, основанных на использовании СБШ, повышать за счет последовательного использования методов линейной и нелинейной рандомизации исходных сообщений, выполняемых перед процедурой блочного шифрования и не вносящих каких-либо изменений непосредственно в алгоритм СБШ.

Вместе с тем, если задача построения линейной части рандомизатора достаточно тривиальна и давно исследована, например в работах [4-6] и многих других, то каким образом построить и смоделировать каскадную схему линейной и нелинейной частей рандомизатора в этих работах не показано. Поэтому данная статья и посвящена построению обобщенной модели такого нелинейного рандомизатора для СБШ, использующего нелинейные взаимно однозначные преобразования в полях Галуа.

Основная часть

Полагаем, что на вход рандомизатора СБШ поступает блок $\bar{s}$ открытого сообщения величиной k бит $(k < n)$:

$$\vec{s} = (s_{k-1}, s_{k-2}, \ldots, s_{i,} \ldots, s_2, s_1, s_0). \quad (1)$$

При этом (как это было указано ранее) процедура рандомизации на входе СБШ должна представлять собой последовательное выполнение двух последовательных преобразований над блоком $\vec{S}$ входного текста.

Во-первых, это линейное преобразование k-битового блока $\vec{S}$ в $(k+l)$-битовый блок $\vec{x}$ с использованием некоторого псевдослучайного параметра t. В свою очередь, параметр t является l-битовым двоичным вектором $\vec{t}$, полученным на выходе генератора псевдослучайных l-битовых чисел.

При этом должно выполняться условие

$$k + l = n. \tag{2}$$

В обобщенной форме можно записать, что

$$\vec{x} = \sigma(\vec{s}, \vec{t}), \tag{3}$$

где σ представляет собой некоторый обобщенный оператор линейного преобразования.

Без потери общности будем считать в дальнейшем, что векторы $\vec{x}$, $\vec{s}$, $\vec{t}$ связаны между собой следующим матричным уравнением

$$\mathbf{A} \cdot \vec{x} = \vec{s}, \tag{4}$$

где матрица $\mathbf{A}$ содержит k строк и $(k+l)$ столбцов.

В этом случае система уравнений (4) является недоопределенной. Решение этой системы можно получить, задав дополнительно некоторые значения для l произвольных компонент вектора $\vec{x}$ из поля $GF(2^n)$ случайным образом с помощью, например, генератора псевдослучайных чисел. В этом случае система (4) станет определенной и будет иметь единственное решение.

Во-вторых, это процедура нелинейного преобразования вектора $\vec{x}$ в вектор

$$\vec{y} = \rho(\vec{x}), \tag{5}$$

где ρ – некоторый обобщенный оператор нелинейного преобразования в поле $GF(2^n)$.

Рассмотрим гипотетический пример. Пусть $k = 5$, $l = 3$, $n = 8$, структура поля $GF(2^8)$ задана неприводимым полиномом

$$m(z) = z^8 \oplus z^4 \oplus z^3 \oplus z \oplus 1, \tag{6}$$

матрица $\mathbf{A}$ линейного преобразования имеет вид

$$\mathbf{A} = \left[\begin{array}{ccccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right], \tag{7}$$

а нелинейное преобразование (5) задано взаимно однозначной функцией

$$\rho(a) = a^{-1},\ \rho(0) = 0. \tag{8}$$

Далее, пусть, например, задан 5-битовый блок открытого сообщения следующего вида:

$$\vec{s} = (1,\ 1,\ 0,\ 1,\ 0). \tag{9}$$

Кроме того, положим, что генератор псевдослучайных чисел выдал 3-битовый случайный вектор

$$\vec{t} = (1,\ 1,\ 1). \tag{10}$$

Тогда система уравнений (4) примет вид

$$\left[\begin{array}{ccccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right] \cdot \begin{pmatrix} x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \tag{11}$$

решая которую в поле $GF(2^8)$ получим

$$\bar{x} = (0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1). \tag{12}$$

Полученный вектор $\bar{x}$ необходимо преобразовать по правилам поля $GF(2^8)$ в вектор $\bar{y} = \rho(\bar{x})$, где оператор ρ определяется согласно выражению (8).

Для нахождения $\rho(\bar{x})$ заметим, что в соответствии с найденным в (12) значением вектора $\bar{x}$ полином $x(z)$ будет иметь следующий вид:

$$\begin{aligned} x(z) &= 0 \cdot z^7 \oplus 1 \cdot z^6 \oplus 0 \cdot z^5 \oplus 0 \cdot z^4 \oplus 0 \cdot z^3 \oplus \\ &\oplus 1 \cdot z^2 \oplus 1 \cdot z^1 \oplus 1 \cdot z^0 = z^6 \oplus z^2 \oplus 1. \end{aligned} \tag{13}$$

Для выполнения операции

$$y(x) = x^{-1}(z) = \frac{1}{z^6 \oplus z^2 \oplus z \oplus 1} \tag{14}$$

в поле $GF(2^8)$ можно использовать любые известные методы или доступные средства, например пакет «GF» из компьютерной системы символьных вычислений Maple [7].

В частности, выполнение операции $y := G[`/`](1, x)$ в этом пакете дает значение

$$x(z)^{-1} = z^6 \oplus z^5 \oplus z^3 \oplus 1. \tag{15}$$

Соответствующий этому полиному двоичный вектор имеет вид

$$\rho(x) = (0,\ 1,\ 1,\ 0,\ 1,\ 0,\ 0,\ 1)^T. \qquad (16)$$

Итак, процедура обобщенной нелинейной рандомизации СБШ (последовательных операций линейной и нелинейной частей рандомизатора) в конструктивном плане описывается следующим образом:

1. Параметрами процедуры, которые должны быть заданы до начала ее выполнения, являются: структура поля $GF(2^n)$; конкретный вид оператора линейного преобразования σ в поле $GF(2^n)$; конкретный вид оператора нелинейного преобразования ρ в поле $GF(2^n)$; характеристики генератора псевдослучайных чисел.

2. Входными переменными процедуры является k-битовое значения блока $\bar{S}$ открытого сообщения S. Кроме того, к входным переменным будем относить и l-битовое значение случайного вектора $\bar{t}$.

3. Выполнение процедуры нелинейной рандомизации представляет собой последовательность двух преобразований в поле $GF(2^n)$:

$$\begin{aligned} \bar{x} &:= \sigma(\bar{s}, \bar{t}); \\ \bar{y} &:= \rho(\bar{x}). \end{aligned} \qquad (17)$$

4. Выходной переменной процедуры является n-битовый $(n = k + l)$ вектор $\bar{y}$, соответствующий полиному $y(z) = \rho(x(z))$.

Все вышеизложенное представляет собой обобщенный случай процедуры нелинейной рандомизации на основе использования линейного и нелинейного преобразований.

Следует отметить, что выполнение линейной части процедуры рандомизации в поле $GF(2^n)$ в нашем случае может быть сведено к решению системы линейных алгебраических уравнений с постоянными целочисленными коэффициентами, значения которых являются элементами множества {0, 1}.

Решение таких систем не вызывает трудностей и может быть получено любым известным способом. Сразу отметим, что вопросы алгоритмической сложности решения подобных систем уравнений и операций обращения матриц в настоящей работе сознательно не рассматриваются, т.к. эти вопросы глубоко проработаны в научно-технической литературе, например [8].

В то же время выполнение нелинейного взаимно однозначного преобразования в поле $GF(2^n)$ в общем случае не является тривиальной процедурой. Однако автором доказана возможность сведения такой задачи к задаче формирования и решения системы алгебраических уравнений с переменными коэффициентами.

Суть предложенного подхода состоит в переходе к обратной задаче нелинейного преобразования в поле $GF(2^n)$ и замене степеней, превышающих n, эквивалентными полиномами степени не выше чем n. Отличительной

чертой предложенного подхода является то, что гарантия существования и единственности решения сформированной системы алгебраических уравнений с переменными коэффициентами является прямым следствием свойств полей Галуа, что, в свою очередь, позволяет использовать для решения данной задачи известные методы линейной алгебры без дополнительных доказательств.

Установлена возможность использования метода последовательных исключений (метода Гаусса) для реализации решения системы уравнений, эквивалентной обратной задаче нелинейного взаимно однозначного разрядного преобразования в полях Галуа, особенностью которой является то, что при любых конкретных значениях вектора входных данных и любых линейных преобразованиях над системой ее коэффициенты принимают целые значения из множества {0, 1}. А это, в свою очередь, означает, что ее решение будет целочисленным, а элементы вектора решения также будут принимать целые значения из множества {0, 1}.

Выводы

В данной работе представлены теоретико-практические подходы к построению обобщенной модели рандомизаторов, основанных на линейных и нелинейных разрядных преобразований в полях Галуа $GF(2^n)$ и используемых для повышения криптостойкости систем криптографической защиты информации (КЗИ) на основе СБШ.

Следует отметить, что в качестве гипотетического примера в работе рассмотрен обобщенный подход к построению модели нелинейного рандомизатора для СБШ с длиной блока $n = 8$ бит, т.е. в поле Галуа $GF(2^8)$. Однако в современных схемах КЗИ в основном используются СБШ, где длина блока равна 64...512 бит и, следовательно, преобразования необходимо производить в полях Галуа высокой размерности – $GF(2^{64})...GF(2^{512})$. Поэтому определение подходов к заданию соответствующей структуры поля и нахождению неприводимых полиномов для этих полей являются отдельной задачей, которая выходят за рамки этой работы и требует проведение дальнейших исследований.

1. *Алексейчук А.Н.* Достаточные условия стойкости рандомизированных блочных систем шифрования относительно метода криптоанализа на основе коммутативных диаграмм // Реєстрація, зберігання і обробка даних. – 2007. – Т. 9. – № 2 – С. 61-68.

2. *Алексейчук А.Н.* Метод построения и теоретико-информационный анализ стойкости рандомизированных криптосистем с секретным ключом / А.Н. Алексейчук, И.В. Васюков, А.В. Корнейко // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 22. – К.: 2003. – С. 65-73.

3. *Алексейчук А.Н.* Обоснование стойкости вероятностных моделей рандомизированных блочных шифров к методу разностного криптоанализа / А.Н. Алексейчук, И.В. Васюков, А.В. Корнейко // Электронное моделирование. – 2004. – Т. 26. – № 4. – С. 23-35.

4. *Rivest R.L., Sherman A.T.* Randomization encryption techniques // Advances in Cryptology – CRYPTO'82, Proceedings. – Springer Verlag, 1982. – P. 145-167.

5. *Massey J.L.* An Introdution to Contemporary Cryptology // Proc. IEEE. – 1988. – Vol. 76, N 5. – P. 533-549.
6. *Maurer U.M.* Provable Security in Cryptography: Diss. ETH N 9260. – 1990. – 120 p.
7. *Дьяконов В.П.* Maple 10/11/12/13/14 в математических расчетах. – М. : ДМК-Пресс, 2011. – 800 с.
8. *Ахо А.* Построение и анализ вычислительных алгоритмов / А. Ахо, Дж. Хопкрофт, Дж. Ульман. – М. : Мир, 1979. – 535 с.

Поступила 6.10.2016 р.

УДК 621.56 : 629.7

А.А. Чирва, г.Киев

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ГИДРАВЛИЧЕСКИХ ПРОЦЕССОВ В ПНЕВМАТИЧЕСКОМ ТРУБОПРОВОДЕ

Abstract. The article presents the basic equations for the pneumatic pipeline, which can be used for transient simulation of hydraulic processes in the plane pneumatic system.

Введение. Регулирование параметров воздуха в пневматической системе самолета (расход, давление) осуществляется различной трубопроводной арматурой, устанавливаемой в системе. Управление данными устройствами осуществляет электронный блок управления системой. По информации, полученной от датчиков в системе, а также от других самолетных систем, блок управление выдает управляющие импульсы на регулирующие устройства в соответствии с заложенными алгоритмами. Так как регулирующее устройство и датчики размещаются в различных местах системы, а также сама магистраль имеет определенный объем, изменение регулируемого параметра в месте установки датчика после выдачи команд на регулирующее устройство происходит с задержкой. Указанные задержки влияют на процесс регулирования, что может привести к автоколебаниям и выходу системы на не рабочие режимы работы. Поэтому актуальным является создание модели динамических переходных процессов в трубопроводе произвольной длины, чему посвящено данное исследование.

Основные допущения и уравнения.

Трубопровод разбивается n расчетных ячеек. Принимаем следующие допущения:

- рассматривается воздух как идеальный газ;
- теплообмен отсутствует;
- отсутствие внутренних источников тепла;