УДК 004.056.57:656.2

С.И. Приходько, Г.С. Цымбал

Украинская государственная академия железнодорожного транспорта, Харьков

МЕТОД ПОЛУЧЕНИЯ НЕЛИНЕЙНЫХ ФУНКЦИЙ ДЛЯ АЛГОРИТМОВ ПОТОЧНОГО ШИФРОВАНИЯ ДАННЫХ

В работе рассмотрены требования к функциям, которые формируют узел нелинейных замен алгоритмов поточного шифрования, приведен анализ существующих методов получения нелинейных эластичных функций, описывается метод получения нелинейных эластичных функций для формирования узлов нелинейных замен алгоритмов поточного шифрования данных.

Ключевые слова: *узел нелинейных замен, нелинейность, эластичность, сверточные коды.*

Введение

Постановка проблемы. Последние исследования в области стойкости криптографических средств защиты информации к современным методам криптоанализа [1 - 3] показывают, что уязвимым является блок нелинейных замен. В Украине нет единого стандара поточного шифрования данных, в данный момент для поточного шифрования применяется ДСТУ ГОСТ 28147:2009 в режиме гаммирования, который является переизданием ГОСТ 28147-89. Криптоанализ последнего показывает, что он морально устарел, и не отвечает современным требованиям по запасу стойкости [1]. Поэтому разработка методов формирования нелинейных замен с улучшенными криптографическими показателями является актуальной задачей.

Анализ последних исследований и публикаций. Узлы нелинейных замен строятся на математическом аппарате булевых функций. Исследования криптографической стойкости современных узлов нелинейных замен показывают, что они демонстрируют низкие динамические и корреляционные свойства, не имеют запаса стойкости [1, 4]. Следовательно, необходимо разработать новые методы формирования узлов нелинейных замен, а именно выбор и/или формирования булевых функций с улучшенными криптографическими показателями. Анализ требований, которые выдвигаются к функциям-кандидатам для формирования узлов нелинейных замен [1], позволяет сделать вывод, что эластичные функции являются наиболее целесообразными для применения. Получение эластичных функций с заданными криптографическими показателями является актуальной задачей [5 – 13]. Анализ методов получения эластичных функций [5 – 8] показывает, что необходима разработка новых методов получения эластичных функций с заданными криптографическими свойствами.

Постановка задачи. На основе анализа требований к функциям-кандидатам для формирования узлов нелинейных замен и анализа методов получения эластичных функций, разработать метод получения эластичных функций с заданными криптографическими свойствами.

Основная часть

Узел нелинейных замен представлен на рис. 1 $(a_1, a_2, ..., a_n) \in A$ – входы в узел нелинейных замен, а $(b_1, b_2, ..., b_n) \in B$ – выходы, $F(x)$ – функция реализующая отображение из $(a_1, a_2, ..., a_n)$ в $(b_1, b_2, ..., b_n)$, т.е. $F(x): A \to B$.

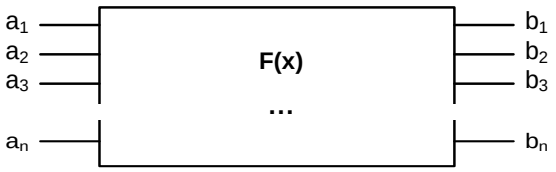

Рис. 1. Узел нелинейных замен

К $F(x)$ предъявляется ряд требований [1], которые обуславливают криптографическую стойкость узла нелинейных замен. Анализ требований позволяет сделать вывод, что эластичные функции являются наиболее целесообразными к применению.

Функция F с n-входом и m-выходом называется (n,m,t)-*эластичной*, если она пробегает все возможные выходные m-векторы равное количество раз в том случае, когда t произвольных входов зафиксировано, а остальные n – t входов пробегают через все 2^{n-t} входных векторов по разу.

Анализ методов получения эластичных функций [5 – 13] позволяет сделать вывод, что наиболее перспективным является метод получения эластичных функций из прототипов - кодов, исправляющих ошибки. А применение в качестве прототипа сверточных кодов позволяет получить такие преимущества: 1) получение полного множества эластичных функций (четное и нечетное m); 2) получение более высоких криптографических показателей за счет характеристических показателей самого кода.

Так как сверточные коды являются бесконечными, и применить матричный способ получения эластичных функций нельзя, необходимо использовать алгебраически заданные сверточные коды.

Метод, который предлагается основан на доказанной взаимосвязи между теорией помехоустойчивого кодирования и эластичными функциями [9, 10]. Так как кодовые слова сверточного кода обладают конструктивными характеристиками самого кода, можно использовать кодовые слова для построения эластичной функции.

Теорема. Пусть P – это (n,k,d) – сверточный код. Тогда можно построить (n,m,t) – эластичную функцию, такую что $k = m$ и $t \le d-1$.

Доказательство. Сверточный код P порождает пространство кодовых слов, которые обладают конструктивными характеристиками самого кода. Доказано [6,9], что для линейного двоичного (n,k,d)-кода с множеством базисных векторов $\vec{u} = (u_0, u_1, ..., u_{n-1})$, для каждого кодового слова $u_i \in P, i = 0,1,...,2^n - 1$ можно сопоставить линейную функцию $l_{u_i} \in L_k$:

$$l_{u_i} = u_i \cdot x = \bigoplus_{r=1}^{k} u_{i,r} x^r$$

Данная линейная функция однозначно определяется u_i. Так как минимальное расстояние P равно d, любая функция l_{u_i} для $u_i \in P$ будет не вырожденной на $d-1$ переменных. Пусть β – примитивный элемент поля $GF(q^z)$, тогда можно записать биективное отображение $\varphi : F_{2^z} \mapsto P$ следующим образом (это задает нам матрицу $2^z - 1 \times z$):

$$A = \begin{pmatrix} \varphi(1) & \varphi(\beta) & \dots & \varphi(\beta^{z-1}) \\ \varphi(\beta) & \varphi(\beta^2) & \dots & \varphi(\beta^z) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi(\beta^{2^z-2}) & \varphi(1) & \cdots & \varphi(\beta^{z-2}) \end{pmatrix}.$$

Используя матрицу A, мы можем построить компонентные функции f_i, связывая соответствующие линейные функции и элемента в i-м столбце матрицы. Из свойств A, следует, что любая комбинация f_i является объединением n линейных функций, которые принадлежат множеству булевых функций B_n, где n – число переменных. Эластичность такой функции $F(f_1,...,f_n)$ равна $t \le \left\lfloor 2^{m-1} n / 2^m - 1 \right\rfloor - 1$. Нелинейность будет равна $N_s(f) = 2^{n-1} - 2^{n-0,5 \cdot m}$. В силу того, что сверточные коды обладают высокими конструктивными характеристиками, это обеспечивает высокие показатели нелинейности и эластичности, а, следовательно, и корреляционного иммунитета полученных эластичных функций.

Таким образом, предложенный метод позволяет получать за одно и то же время эластичные функции, с более высокими криптографическими показателями, чем функции, которые были полученные из блоковых линейных кодов. Это обуславливается конструктивными характеристиками сверточных кодов. А использование алгебраически заданных сверточных кодов позволяет использовать вместо порождающей матрицы кодовые слова сверточного кода.

Выводы

В работе были проанализированы требования к функциям-кандидатам для построения узлов нелинейных замен, подходы к построению эластичных функций. Предложен метод получения эластичных функций с улучшенными показателями криптографической стойкости. Результаты экспериментов показывают, что полученные таким методов эластичные функции проходят проверку на соответствие требованиям к функциям-кандидатам. Показывают существенное преимущество с существующими эластичными функциями по таким показателям, как критерий распространения, нелинейность, корреляционный иммунитет, но уступают по таким показателям, как функция автокорреляции. Таким образом, перспективным направлением дальнейших исследований является постановка многокритериальной задачи выбора сверточного кода, для того ,чтобы эластичная функция, полученная данным методом удовлетворяла всем вышеуказанным требованиям.

Список литературы

1. *Кузнецов А.А. Разработка предложений по совершенствованию симметричных средств защиты информации перспективной системы критического применения / А.А. Кузнецов, И.В. Московченко // Радіоелектронні і комп'ютерні системи. – 2008. – № 2 (29). – С. 94-100.*
2. *Потий А.В. Исследование методов криптоанализа поточных шифров / А.В. Потий, Ю.А. Избенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – ДСТСЗІ СБУ, НТУ «КПІ», 2003. – № 6. – С. 34-49.*
3. *Потий А.В. Системы показателей оценки эффективности функционирования схем поточного шифрования / А.В. Потий, Ю.А. Избенко // Радиотехника: Всеукраинский межведомственный научно-технический сборник. – 2003. – № 123. – С. 146-158.*
4. *Подстановочные конструкции современных симметричных блочных шифров / В.И. Долгов, Р.В. Олейников, И.В. Лисицкая, Р.В. Сергиенко, Е.В. Дроботько, Е.Д. Мельничук // Радіоелектронні і комп'ютерні системи. – 2009. – № 6 (40). – С. 89-93.*
5. *Xian-Mo Zhang. Cryptographically Resilient Functions [Электронный ресурс] / Xian-Mo Zhang, Yuliang Zheng. – Режим доступа к ресурсу: http://pscit-www.fcit.monash.edu.au/ ~yuliang/pubs/ie3it-resi.ps.*
6. *Pascale Charpin Highly Nonlinear Resilient Functions Through Disjoint Codes in Projective Spaces / Pascale Charpin, Enes Pasalic // Design, Codes and Cryptography. – 2005. – № 37. – P. 319-346.*
7. *Stinson D.R. An finite calss of counterexamples to a conjecture concerning non-linear resilient functions [Электронный ресурс] / D.R. Stinson, J.L. Massey. – Режим доступа к ресурсу: http://www.cacr.math.uwaterloo.ca/ ~dstinson/papers/respk.ps.*
8. *Camion Paul. Correlation-Immune and Resilient Functions Over a Finite Alphabet and Their Applications in Cryptography [Электронный ресурс] / Paul Camion, Anne Canteaut. – Режим доступа к ресурсу: http://portal.acm.org/ citation.cfm?id=309154.*
9. *The bit extraction problem or t-resilient functions /*

B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, R. Smolensky // In 26th IEEE Symposium on Foundations of Computer Science. – 1985. – P. 396-407.

10. Bennet C.H. Privacy amplification by public discussion / C.H. Bennet, G. Brassard, J.M. Robert // SIAM Journal on Computing, – 1988. – Vol. 24. – P. 210-229.

11. Seberry J. Pitfalls in Designing Boxes (Extended Abstract) / J. Seberry, X.M. Zhang, Y. Zheng // Springer–Verlag. – 1998. – P. 383-396.

12. Xiao G.Z. A spectral characterization of correlation-immune functions / G.Z. Xiao and J. L. Massey // IEEE Trans. Inform. Theory. – May 1988. – Vol. 34, no. 3. – P. 569-571.

13. Поточные шифры. Результаты зарубежной открытой криптологии [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm.

Поступила в редколлегию 21.04.2011

Рецензент: д-р техн. наук, проф. Г.В. Альошин, Украинская государственная академия железнодорожного транспорта, Харьков.

МЕТОД ОТРИМАННЯ НЕЛІНІЙНИХ ФУНКЦІЙ ДЛЯ АЛГОРИТМІВ ПОТОКОВОГО ШИФРУВАННЯ ДАНИХ

С.І. Приходько, Г.С. Цимбал

У роботі розглянуті вимоги до функцій, які формують вузол нелінійних замін алгоритмів потокового шифрування, проведено аналіз існуючих методів отримання нелінійних еластичних функцій, описується метод отримання нелінійних еластичних функцій для формування вузлів нелінійних замін алгоритмів потокового шифрування даних.

***Ключові слова**: вузол нелінійних замін, нелінійність, еластичність, згортальні коди.*

METHOD OF RECEIPT OF NONLINEAR FUNCTIONS FOR THE ALGORITHMS OF STREAM ENCRYPTION OF DATA

S.I. Pryhodko, G.S. Tsymbal

In abstract requirements to the functions which form the block of nonlinear replacements of algorithms of stream encryption are considered, an analysis over of existent methods of obtaining of nonlinear resilient functions is considered, the method of obtaining of non-linear resilient functions for formation of block of non-linear changeovers of algorithms of stream encryption of the data is described.

***Keywords:** block of nonlinear replacements, nonlinearity, resiliency, convolutional codes.*