УДК 004.056.2

М. О. Алексеев

НОВАЯ КОНСТРУКЦИЯ СИСТЕМАТИЧЕСКОГО НАДЕЖНОГО КОДА

Предложена конструкция систематического надежного кода. Представлена новая нелинейная функция для вычисления проверочных символов кода. Проанализирована надежность кода при обнаружении однонаправленных ошибок.

Ключевые слова: *нелинейная функция, надежный код, однонаправленные ошибки, показательная функция.*

Введение. Появление криптоатак, ориентированных на особенности реализации криптографических алгоритмов, требует разработки методов проектирования защищенных архитектур вычислительных устройств. Такие криптоатаки, получившие название „атаки по сторонним каналам“, основаны на сборе и анализе информации о физических особенностях криптографических модулей (как аппаратных, так и программных) [1, 2].

Одну из основных угроз для криптографических модулей представляют помехи, индуцируемые злоумышленником. Анализ работы устройства в условиях помех предоставляет атакующему дополнительную информацию, которая может быть использована для успешного взлома шифра [3].

Дублирование оборудования с последующим сравнением результатов его работы не обеспечивает надежной защиты от атак с привнесением помех. Если злоумышленник способен возбуждать помехи с достаточно высоким пространственным и временным разрешением, то наложение одинаковых помех на оба экземпляра атакуемого блока (исходного и дублирующего) приведет к необнаруживаемой ошибке на выходе устройства. Очевидно, что даже многократного дублирования защищаемого блока недостаточно в такой ситуации.

Линейные помехоустойчивые коды, часто применяемые в аппаратных схемах для контроля ошибок, также не обеспечивают необходимый уровень защиты устройства. Если злоумышленник способен контролировать возникающие ошибки, то, генерируя помехи, приводящие к любой из $q^k - 1$ необнаруживаемых ошибок, соответствующих ненулевым кодовым словам, он обеспечивает ошибочный выход атакуемого блока вне зависимости от поступающих данных.

Надежные коды. Обеспечить защиту от описанной модели атаки позволяют нелинейные коды. Коды, названные надежными, обеспечивают обнаружение любой ошибки с заданной вероятностью. В настоящей работе приведено лишь определение надежных кодов; более подробно эти коды приведены в работах [4—6].

Пусть $C \in GF(p^n)$ является (n, M)-кодом, где $M = |C|$.

Код C называется надежным по отношению к его вероятности обнаружения ошибки, если вероятность $Q(e)$ необнаружения ошибки e меньше единицы для всех ненулевых e:

$$Q(e) = \frac{|\{w \mid w \in C, w+e \in C\}|}{|C|} < 1,\ e \neq 0,$$

где $w, e \in GF(p^n)$.

Через R обозначается мощность максимального пересечения кода C и его сдвигов $C+e$, $e \in GF(p^n)$, $e \neq 0$. Другими словами, R — максимальное число кодовых слов кода C, при наложении на которые фиксированной ошибки $e \neq 0$ получаются кодовые слова. Очевидно, что в этом случае ошибка не может быть обнаружена. Отсюда следует, что вероятность обнаружения ошибки P_{det} ограничена снизу выражением $P_{\text{det}} \geq 1 - R/M$, т.е. любая ошибка может быть обнаружена с вероятностью не ниже $1 - R/M$.

Над полем с характеристикой $p > 2$ может быть построен код, у которого $R = 1$. В случае, когда $p = 2$ (наиболее востребовано с точки зрения реализации), минимальным возможным параметром является $R = 2$ [4].

На практике наиболее удобно использовать систематические коды, так как при защите аппаратных блоков требуется высокая скорость обработки данных.

Согласно теореме 2 из работы [5], конкатенация информационной $x \in GF(2^k)$ и проверочной $y = f(x)$, $y \in GF(2^r)$ части образует кодовые слова $(x \mid y = f(x))$ надежного систематического кода, параметры которого определяются следующим образом: $R = 2^k P_f$, $n = k + r$, $|M| = 2^k$. Параметр P_f определяет степень нелинейности функции.

Надежные коды используются как для защиты криптографических модулей, так и для защиты систем хранения. Избыточность, необходимая для защиты аппаратных схем, заключается в дублировании оборудования и добавлении блоков вычисления проверочных символов. В случае проектирования защищенного модуля памяти размер требуемой памяти увеличивается в n/k раз.

Нелинейная показательная функция. Согласно статье [7], функция $f(x) = u^x \bmod p$ (где x — элемент абелевой группы $G = \{0, ..., p-1\}$, p — простое число, а u — элемент порядка q из поля $GF(p)$) является разностно $\left(\frac{p-1}{q} + 1\right)$-равномерным отображением.

Исследуем степень нелинейности этой функции. Пусть $a,\ b \in G$ и $a \neq 0$. Тогда уравнение

$$u^{(x+a) \bmod p} - u^x = b \tag{1}$$

эквивалентно

$$\begin{cases} u^{x+a} - u^x = b \text{ и } 0 \leq x \leq p-a-1 \\ \text{или} \\ u^{x+a-p} - u^x = b \text{ и } p-a \leq x \leq p-1. \end{cases} \tag{2}$$

Из уникальности решения x уравнения

$$u^{x+a} - u^x = b$$

по модулю q следует, что первое уравнение (2) имеет не более $\left\lceil \frac{p-a}{q} \right\rceil$ корней в G, второе — не более $\left\lceil \frac{a}{q} \right\rceil$. Следовательно, уравнение (1) имеет не более

$$\left\lceil \frac{p-a}{q} \right\rceil + \left\lceil \frac{a}{q} \right\rceil = \frac{p-1}{q} + 1$$

решений в G.

Выбрав в качестве u примитивный элемент поля $GF(p)$, можно получить из (1) уравнение вида $f(x+a)-f(x)=b$, которое имеет не более двух корней. Оно аналогично проверочному выражению надежных кодов. С помощью этого соотношения определяется наличие ошибок.

Стоит отметить, что при использовании в качестве u примитивного элемента поля $f(x)=u^x \bmod p$ становится почти совершенно нелинейной функцией с $P_f = 2/p$.

Таким образом, конкатенацией информационной x и проверочной части $y=u^x \bmod p$ получаем систематический надежный код со следующими параметрами: $k=\lceil \log_2 p \rceil$, $r=k$, $n=2k$, $R=2$.

Однонаправленные атаки. Известные 2-надежные коды в качестве совершенно нелинейных используют степенные функции и функцию инвертирования в поле [6]. Эти коды являются надежными с заданной вероятностью обнаружения ошибок при аддитивной модели помехи.

Однако не всегда ошибки в устройстве могут быть описаны аддитивной моделью. Как показывает практика, для flash-памяти, оптических дисков и сетей характерна достаточно большая разница между вероятностями переходов $0 \to 1$ и $1 \to 0$ [8]. Зачастую используется допущение, что в таких системах возможен только один тип переходов. Подобные ошибки получили название асимметричных.

Исследования показали, что для некоторых систем хранения (LSI/VLSI ROM и RAM) характерны однонаправленные ошибки, отличающиеся от асимметричных тем, что оба перехода $0 \to 1$ и $1 \to 0$ возможны, но в каждом отдельном слове встречается только один тип перехода — один тип асимметричной ошибки. Математически такая ошибка может быть представлена как побитовая конъюнкция/дизъюнкция кодового слова c и некоторого вектора w, состоящего из нулей и единиц: переход $0 \to 1$ — $c \vee w$; переход $1 \to 0$ — $c \wedge w$.

При индуцировании помех криптоаналитиком (искусственном происхождении ошибки) также возможны асимметричные и однонаправленные модели ошибок. Возможность осуществлять переход всех битов в 0 позволяет криптоаналитику успешно внедрять необнаруживаемые ошибки даже при использовании существующих надежных кодов.

Рассмотрим пример. Для защиты блока памяти используется 2-надежный код $(x \mid y = x^3)$ над полем $GF(p^n)$. Допустим, злоумышленник осуществил атаку, которая привела к переходу $0 \to 0$, $1 \to 0$ для всех битов кодового слова. Тогда проверочное уравнение $f(x \wedge 0) = f(x) \wedge 0$ при $f(x)=x^3$ будет выполняться при любых x и атака не будет обнаружена. Аналогична ситуация и для функции инвертирования в поле, так как она доопределяется тем, что $0^{-1}=0$ [5].

Предлагаемая конструкция кода обеспечивает защиту даже при однонаправленных ошибках. Это обеспечивается тем, что в общем случае $u^0 \neq 0$ и $u^{p-1} \neq p-1$.

Наиболее эффективным сценарием криптоатаки на данный надежный код представляется приведение данных к кодовым словам наименьшего или наибольшего веса Хемминга (в зависимости от типа перехода ошибки). Например, наименьшим весом обладает слово $(0 \mid u^0 = 1)$. Злоумышленник может обнулить все биты информационной части кодового слова, а у проверочной части оставить нетронутым только младший бит. Далее, в зависимости от значения младшего бита выполняется (1) или не выполняется (0) проверочное соотношение. Таким образом, вероятность необнаружения ошибки при однонаправленной атаке ограничена сверху значением 0,5 (при равномерном распределении сообщений). Тут необходимо отме-

тить, что для успешного проведения большинства типов атак с привнесением ошибок требуется внедрение заданного количества необнаруженных ошибок. В такой ситуации вероятность необнаружения ошибки убывает экспоненциально с ростом числа атак.

Таким образом, предлагаемый код обеспечивает надежную защиту не только от ошибок и атак, описываемых аддитивной моделью, но и от воздействий, описываемых моделью однонаправленных ошибок.

Практическая значимость. Очевидно, что процедуры кодирования и декодирования предлагаемого кода обладают более высокой вычислительной сложностью, нежели существующие кодовые конструкции. Однако если криптографический модуль использует алгоритм Диффи—Хеллмана для генерации секретного ключа между двумя устройствами, то модули, выполняющие возведение в степень по модулю простого числа, могут быть использованы и для процедур кодирования и декодирования предлагаемого кода. Более того, в обоих случаях требуется возведение фиксированного основания в степень, значение которой является переменной величиной. Поэтому могут быть применены эффективные алгоритмы возведения в степень по модулю простого числа, например, метод Евклида для фиксированного основания [9].

Также возможно эффективное использование данного надежного кода в криптографических модулях, использующих возведение в степень при шифровании и дешифровании, примерами являются шифры RSA и Эль-Гамаля, а также электронные цифровые подписи на их основе. Использование уже реализованных в устройстве блоков сводит аппаратные затраты к минимуму.

СПИСОК ЛИТЕРАТУРЫ

1. *Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К.* Использование помехоустойчивых кодов для шифрации видеоинформации // ИУС. 2007. №5(30). С. 23—26.

2. *Zhou Y., Feng D.* Side-channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. 2005 [Электронный ресурс]: <http://eprint.iacr.org/2005/388/>.

3. *Biham E., Shamir A.* Differential Cryptanalysis of DES-like Cryptosystems. The Weizmann Institute of Science, Department of Applied Mathematics, 1990.

4. *Akdemir K. D., Wang Z., Karpovsky M. G., Sunar B.* Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes // Fault Analysis in Cryptography. 2011.

5. *Kulikowski K., Karpovsky M. G.* Robust Correction of Repeating Errors by Nonlinear Codes // Communications, IET. 2011. Vol. 5, N 4. P. 2317—2327.

6. *Karpovsky M. G., Kulikowski K., Wang Z.* On-line self error detection with equal protection against all errors // Int. J. of Highly Reliable Electronic System Design. 2008.

7. *Nyberg K.* Differently uniform mappings for cryptography // Eurocrypt 1993. Lecture Notes in Computer Science. 1994. Vol. 765. P. 55—64.

8. *Ahlswede R., Aydinian H., Khachatrian L.* Unidirectional error control codes and related combinatorial problems // Proc. 8th Intern. Workshop Algebr. Combin. Coding Theory (ACCT-8). St. Petersburg, 2002. P. 6—9.

9. *Menezes A., van Oorschot P., Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1996.

Сведения об авторе

Максим Олегович Алексеев — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра аэрокосмических компьютерных технологий; E-mail: alexeevmo@gmail.com

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.