УДК 004.056.2

М. О. Алексеев

НИЖНЯЯ ГРАНИЦА ДЛИНЫ СИСТЕМАТИЧЕСКИХ РАВНОМЕРНО НАДЕЖНЫХ КОДОВ

Приведены основные определения надежных кодов, обнаруживающих ошибки, указана область их применения. Выведена нижняя граница длины систематических R-равномерно надежных кодов.

Ключевые слова: *нелинейный код, надежный код, нижняя граница, минимальная длина кода.*

Аппаратные реализации криптографических алгоритмов могут быть уязвимы к так называемым атакам по сторонним каналам [1, 2]. Такие атаки основаны на изучении и последующем анализе физических особенностей работы криптосхем, что может привести к вычислению секретного ключа. Анализируемые характеристики аппаратной реализации могут быть

различны: энергопотребление, время выполнения операций, работа схемы в условиях воздействия помех.

В работе [3] описан метод дифференциального криптоанализа, позволяющий вычислять значение секретного ключа, если возможно задать разности между входными последовательностями на определенных этапах блокового DES-подобного шифра. Этот метод применяется для большинства симметричных блоковых шифров, включая AES (например, [4]).

Одну из наиболее серьезных угроз для криптосхем представляет комбинирование атаки с привнесением помех и дальнейшего дифференциального анализа. Внося помехи в определенные участки схемы, злоумышленник может контролировать выходы атакуемых блоков алгоритма, что значительно увеличивает вероятность успешного взлома устройства [5].

В ситуации, когда атакующий контролирует возникающие в устройстве ошибки, классические методы защиты аппаратных схем, основанные на дублировании оборудования и использовании линейных помехоустойчивых кодов, не могут обеспечить требуемый уровень защиты информации. Преодолеть эту проблему позволяют надежные коды, обнаруживающие ошибки. Использование таких кодов дает возможность значительно снизить вероятность успешного проведения рассматриваемой атаки.

Надежные коды также могут применяться в каналах, в которых конфигурация возникающих ошибок не может быть предсказана заранее, например, в системах, подверженных воздействию радиации, заряженных частиц и других факторов. Кроме того, надежные коды, обнаруживающие ошибки, применяются в схемах надежного разделения секрета и смежных с ними областях [6].

Надежным называется код, для которого не существует необнаруживаемых ошибок, т.е. любая ошибка выявляется с заданной вероятностью.

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

Определение 1. Код C называется *надежным*, если значение вероятности $Q(e)$ 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 $w, e \in GF(p^n)$.

На практике наиболее востребованы систематические надежные коды, поскольку они обеспечивают минимальную задержку декодирования — это является одним из основных требований к проектированию аппаратных схем. В настоящей статье рассматриваются только систематические коды, для длины которых и будет выведена нижняя граница.

Определение 2. Код C называется *равномерно надежным* к вероятности обнаружения ошибки, если вероятность $Q(e)$ постоянна и не зависит от ненулевого вектора e:

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

Равномерно надежные коды достаточно хорошо изучены, это наиболее используемый вид надежных кодов благодаря простоте их построения. Проверочные символы таких кодов вычисляются с помощью нелинейных функций, при этом кодовое слово c представляет собой конкатенацию информационной части x и проверочных символов $y = f(x)$, где $f(\cdot)$ — используемая нелинейная функция. Более подробно эти коды описаны в работе [7]. На данный момент хорошо исследованы классы функций, обладающих высокой степенью нелинейности [8].

Определение 3. *R-надежным кодом* называется код, у которого $R = \max |\{w \mid w \in C, w + e \in C\}|$ для всех $e \neq 0$.

Очевидно, что вероятность обнаружения ошибки для *R*-равномерно надежного кода определяется как $P_{\text{det}} = 1 - R/M$.

Необходимо отметить, что для кодов над полем с характеристикой 2 наименьшим достижимым значением *R* является 2 (в силу идентичности операций сложения и вычитания), для других полей — $R = 1$.

Исследуем минимальную длину (обозначим ее через *n*) систематического *R*-равномерно надежного кода. Пусть *k* — размерность кода, т.е. $p^k = M$. В силу равномерной надежности кода число различных разностей между кодовыми словами составляет $\frac{M(M-1)}{R}$. Каждая из этих разностей является элементом поля $GF(p^n)$, над которым построен код. Следовательно, поле должно содержать не менее $\frac{M(M-1)}{R}$ элементов. Кроме того, для систематического кода p^{n-k} элементов поля не могут быть разностями между кодовыми словами, потому что разность систематических частей кодовых слов не может равняться $0 \in GF(p^k)$. Для такого кода только $p^n - p^{n-k}$ элементов поля могут являться разностями кодовых слов, и их должно быть не менее $\frac{M(M-1)}{R}$. Из этого утверждения можно получить нижнюю границу длины систематического *R*-равномерно надежного кода:

$$p^n - p^{n-k} \geq \frac{M(M-1)}{R},$$

$$p^n(1 - p^{-k}) \geq \frac{M(M-1)}{R},$$

$$P^n\left(\frac{M-1}{M}\right) \geq \frac{M(M-1)}{R},$$

$$p^n \geq \frac{M^2}{R},$$

$$n \geq \left\lceil \log_p \frac{M^2}{R} \right\rceil.$$

Легко заметить, что при $p = 2$ и $R = 2$ $n \geq 2k - 1$. При $k = 2$ ($n \geq 2k - 1 = 3$) примерами кодов, лежащих на этой границе, являются $C_1 = \{(00|1), (01|0), (10|0), (11|1)\}$ и $C_2 = \{(00|0), (01|1), (10|1), (11|1)\}$ над $GF(2^3)$, где символ „|“ разделяет информационную и проверочную части слова соответственно. Данные коды являются равномерно надежными систематическими с $R = 2$ и $Q(e) = 1 - 2/4 = 0,5$, являясь при этом кодами с минимальной возможной длиной.

Для сравнения, в работе [9] были предложены конструкции кодов над полем $GF(2^n)$ с $R = 2$ для любых *k*. Коды такой конструкции обладают скоростью $1/2$, т.е $n = 2k$. Представленные коды C_1 и C_2 для $k = 2$ обладают меньшей избыточностью при сохранении той же вероятности обнаружения ошибки $P_{\text{det}} = 0,5$.

Данная граница может быть использована для оценки вводимой избыточности надежных кодов. Условие применимости данной границы следующее: параметр *R* должен делить величину *M*(*M*–1). В общем случае задача построения оптимальных надежных кодов, соответствующих нижней границе, является открытой.

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. *Koeune F., Quisquater J. J.* Side Channel Attacks. Scientific Report. K2Crypt, 2002.

3. *Biham E., Shamir A.* Differential Cryptanalysis of DES-like Cryptosystems. The Weizmann Institute of Science, Department of Applied Mathematics. July 19, 1990.

4. *Dusart P., Letourneux G., Vivolo O.* Differential Fault Analysis on AES // Cryptology ePrint Archive. Report 2003/010.

5. *Kulikowski K. J., Karpovsky M. G., Taubin A.* Robust Codes and Robust, Fault Tolerant Architectures of the Advanced Encryption Standard // J. of System Architecture. 2007. Vol. 53. P. 138—149.

6. *Cramer R., Dodis Y., Fehr S., Padry C., Wichs D.* Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors // Advances in Cryptology. Eurocrypt Lecture Notes in Computer Science. 2008. Vol. 4965. P. 471—488.

7. *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.

8. *Тужилин М. Э.* Почти совершенные нелинейные функции // ПДМ. 2009. № 3. С. 14—20.

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

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.