Модели функционирования персональных систем идентификации с процедурами помехоустойчивого кодирования

10, октябрь 2012

DOI: 10.7463/1012.0486630

Крюков Д. А.

УДК 004.3

Россия, МГТУ МИРЭА

dm.bk@bk.ru

Введение

Сегодня трудно представить развитие телекоммуникационной отрасли без широкого применения SMART-карт, банковских пластиковых карт, RFID-устройств, чип ключей автомобиля, биометрического паспорта. При этом, перечислена лишь часть устройств, которая имеется в постоянном пользовании практически у каждого. Список подобных устройств можно продолжить, с каждым годом появляются новые образцы, более портативные, более производительные. В настоящее время все перечисленные персональные устройства идентификации (ПУИ) реализуют крайне важную функцию, они являются носителями исключительных данных владельца. Ввиду наибольшей (по сравнению со всеми остальными автоматизированными устройствами) приближенности к различным общественным процессам и непосредственно к человеку (владельцу) ценность информации в таких устройствах намного превышает их рыночную стоимость [1]. Потеря или искажение информации являются критичными и не допустимы для них. Таким образом, долговременное хранение и своевременное предоставление информации является ключевой функцией каждого персонального устройства идентификации. На базе моделей функционирования систем идентификации и моделей получения информации из памяти устройств представляется возможным провести анализ возможностей повышения надежности таких устройств в части хранения и предоставления информации путем использования кодов коррекции ошибок.

Системы идентификации

Основными элементами любой системы идентификации помимо персонального устройства идентификации, являются интерфейсное устройство и канал связи между ними [2]. Процедуры помехоустойчивого кодирования и декодирования информации, хранимой в ПУИ, могут осуществляться либо интерфейсным устройством, либо непосредственно устройством. Кроме того, в случае SMART-карт могут также выполняться процедуры шифрования и дешифрования данных, а также процедуры помехоустойчивого кодирования данных перед передачей их по каналу связи, и соответствующее декодирование.

Возможны две основные схемы функционирования систем идентификации. Первая из них изображена на рисунке 1.

Рис. 1. Вариант функционирования системы идентификации в случае коррекции на стороне интерфейсного устройства

При такой схеме функционирования, после чтения закодированных данных, хранящихся в памяти устройства идентификации, происходит их декодирование на интерфейсном устройстве. В случае обнаружения ошибки, данные должны быть скорректированы и вновь отправлены в персональное устройство для перезаписи. В случае если устройство идентификации предусматривает только чтение данных, без их перезаписи, схема упрощается путем удаления из нее процедур кодирования и записи. Но в этом случае, обнаружение ошибки при декодировании будет указывать на необходимость замены устройства.

Вторая схема функционирования может быть реализована только для устройств с чипом (в частности: SMART-карт, микропроцессорных RFID-меток, биометрических паспортов и т.п.) и заключается в размещении всех процедур помехоустойчивого кодирования и декодирования данных в самой карте. Данная схема функционирования изображена на рис. 2.

Рис. 2. Вариант функционирования системы идентификации в случае коррекции на стороне устройства идентификации

Так как такая схема функционирования возможна только для устройств с чипом, в нее должны быть также помещены процедуры шифрования и дешифрования передаваемых данных, а также процедуры кодирования данных перед передачей по каналу связи и декодирования. Следовательно, вторая схема функционирования в действительности будет иметь вид, показанный на рисунке 3.

Рис. 3. Вариант функционирования системы идентификации в случае коррекции на стороне устройства идентификации

Блоки «Кодирование 2» и «Декодирование 2» обозначают процедуры помехоустойчивого кодирования, применяемые при передаче данных. В качестве таковых могут выступать как простые контрольные суммы (например, проверка на четность), так и различные циклические коды. Блоки «Кодирование 1» и «Декодирование 1» обозначают процедуры, применяемые при хранении данных в памяти персональных устройств идентификации.

Помимо представленных схем функционирования другими возможными вариантами являются схемы, в которых процедуры кодирования и декодирования реализуются в различных элементах системы.

Проведем анализ обозначенных схем функционирования систем идентификации по следующим критериям:

- обеспечение эффективности функционирования системы;
- обеспечение безопасности данных;
- обеспечение целостности данных.

Рассмотрим первую схему функционирования:

Будем предполагать, что интерфейсное устройство обладает достаточной вычислительной мощностью для обеспечения кодирования/декодирования данных за приемлемое время. Поэтому в большой степени эффективность работы системы зависит от канала связи и количества передаваемых по нему данных. Для того чтобы интерфейсное устройство смогло осуществлять кодирование или декодирование данных, ему должен быть передан целый блок данных. Возникает ситуация, когда для проверки или кодирования некоторого набора данных интерфейсное устройство вынуждено запрашивать у персонального устройства идентификации более широкий набор данных. Это обстоятельство накладывает существенное ограничение на разбиение данных, хранимых в памяти устройстве, на блоки кодирования. С целью избежать передачи лишних данных по каналу связи, в каждый блок данных по возможности должны помещаться только данные, используемые всегда вместе.

Другим недостатком данной схемы функционирования является ситуация, когда на код, передаваемый по каналу связи от персонального устройства к интерфейсному, накладывается ошибка во время передачи. Интерфейсное устройство не сможет отличить ее от ошибки хранения данных, и в случае если сможет исправить ее, в устройстве идентификации будет произведена перезапись данных на исходные. В случае неисправимости ошибки будет зафиксирована мнимая неисправимая потеря данных в памяти персонального устройства при их действительной сохранности.

Кроме того, эффективность функционирования системы зависит также от объема избыточной информации. Память устройства идентификации сильно ограничена, и потому должна использоваться максимально эффективно;

Содержание в одном кодовом блоке данных, которые не всегда передаются вместе, приводит не только к излишней загрузке канала связи, но и к потенциальному снижению уровня безопасности. Таким образом, соображения безопасности являются дополнительным аргументом в пользу разделения данных при кодировании на максимально независимые блоки;

В силу предположений интерфейсное устройство обеспечивает достаточную вычислительную мощность для работы любых алгоритмов помехоустойчивого кодирования и декодирования. Поэтому выбор методов помехоустойчивого кодирования ограничивается только объемом памяти устройства идентификации, который можно

«потратить» на избыточную информацию кода. Для конкретных видов персональных устройств могут быть подобраны индивидуальные эффективные методы помехоустойчивого кодирования информации.

Проведем анализ второй схемы функционирования систем идентификации:

При данной схеме функционирования по каналу связи системы идентификации передаются те же данные, что передавались бы без реализации методов помехоустойчивого кодирования хранимых данных. Эффективность системы полностью зависит от реализации процедур кодирования и декодирования в логике персональных устройств идентификации. Данные устройства обладают ограниченной вычислительной мощностью, поэтому важным является построение процедур кодирования и декодирования таким образом, чтобы время, затрачиваемое на них, было минимально и не ощутимо для держателя (не более 1 секунды).

Другим ограничением является внутренняя память устройства идентификации. Во-первых, при программной реализации методов кодирования-декодирования код занимает определенный объем памяти, который не должен быть слишком большим (не более нескольких Кб). Во-вторых, избыточная информация помехоустойчивого кода также как и для первого варианта схемы функционирования может занимать значительный объем памяти устройства. Этот объем не должен превышать каких-то пределов, зависящих от конкретной сферы применения устройства и его аппаратных возможностей;

С точки зрения безопасности, данная схема функционирования является достаточно надежной. Все процедуры помехоустойчивого кодирования и декодирования хранимых данных реализуются в пределах персонального устройства, тем самым оставляя уровень безопасности системы идентификации на прежнем уровне;

В отличие от первого варианта схемы функционирования, помимо ограничения на объем избыточной информации также накладываются ограничения на вычислительную мощность, требуемую алгоритмами кодирования и декодирования. Это существенно ограничивает возможности применения помехоустойчивого кодирования данных устройствами идентификации. Таким образом, разработка эффективных методов кодирования и декодирования для данной схемы реализации значительно сложнее.

Подводя итог проведенному анализу, заключаем, что для устройств, на интегральных микросхемах: SMART-картах, RFID-устройствах с чипом, биометрических паспортов и т.п. наиболее подходящей является схема функционирования, когда процедуры кодирования и декодирования данных размещаются в самом устройстве.

Для карт, в которых носителем данных является магнитная полоса, единственным возможным вариантом является размещение процедур кодирования и декодирования на интерфейсном устройстве.

Модель хранения информации в электронно-стираемого программируемого постоянного запоминающего устройства

Основной задачей помехоустойчивого кодирования является обеспечение восстановления данных, хранившихся в вышедшей из строя странице электронно-стираемого программируемого постоянного запоминающего устройства (ЭСПЗУ), и сохранение их в другой рабочей странице памяти. Работу процедур кодирования/декодирования можно считать эффективной, если будут восстановлены данные хотя бы при первом сбросе одной страницы памяти. В дальнейшем будем рассматривать только ситуацию, когда из строя выходит одна страница памяти.

В соответствии с границей Синглтона [3] для того, чтобы код обладал способностью восстановления одной страницы памяти, необходимо не менее двух страниц с избыточной информацией.

Одним из методов помехоустойчивого кодирования для исправления пакетных ошибок является перемежение и восстановление кода, смысл которого заключается в более равномерном распределении пакетной ошибки по кодовым словам. Данный метод может быть адаптирован для нашей ситуации. А именно, в качестве кодируемых блоков данных можно рассматривать последовательности из i -ых символов кодируемых страниц памяти. Каждый символ представляет какую-то часть данных фиксированной длины. В частности, в качестве таковых могут рассматриваться биты или байты данных страницы, или вся страница может рассматриваться как один символ. Соответствующее разбиение на блоки изображено на рисунке 4:

Кодовые слова:

$$\begin{array}{cccc}
 x_0^0 & x_1^0 & \dots & x_0^{N-1} \\
 x_0^1 & x_1^1 & \dots & x_1^{N-1} \\
 \dots & \dots & \dots & \dots
 \end{array}$$

Рис. 4. Размещение страниц в памяти устройства

Полученные кодовые слова будут содержать в себе не более одной ошибки в случае возникновения сбоя одной из страниц. Поэтому для данных последовательностей данных достаточно будет использовать код, исправляющий одну ошибку. Примером таких кодов могут служить коды Хэмминга и коды Рида-Соломона. Но прежде чем анализировать и сравнивать данные коды для рассматриваемой ситуации, проведем общий анализ предложенной методики кодирования.

С целью сохранения структуры файловой системы и файлов данных, наиболее разумным будет использование систематических кодов. Иными словами, для кодирования данных необходимо резервировать какое-то место в памяти для избыточной информации контроля, а часть памяти с данными оставлять неизменной. Договоримся в дальнейшем называть страницы части памяти с избыточной информацией страницами контроля, а страницы части памяти с данными так и называть страницами данных.

После перезаписи любой из страниц данных должен происходить пересчет контрольных символов кода и перезапись страниц контроля. Логичным будет предположить, что для большинства кодов число страниц контроля значительно меньше числа страниц данных. Это означает, что число циклов стирания/записи для страниц контроля растет значительно быстрее, чем для страниц данных. Наиболее вероятной

является ситуация, что первой страницей памяти ЭСПЗУ, давшей сбой, станет страница контроля.

Исследуем подробнее зависимость числа циклов стирания/записи страниц контроля от распределения процедур записи между страницами данных. Под процедурой записи данных мы будем понимать процедуру записи некоторого числа страниц данных, после которой происходит помехоустойчивое кодирование данных, и запись контрольной информации в страницы контроля.

Модель случайного выбора страниц памяти для записи

Одним из вариантов использования памяти ЭСПЗУ является ситуация, когда запись может происходить многократно в различные страницы памяти. При каждой процедуре записи перезаписывается некоторый набор страниц данных в зависимости от действий, совершаемых в системе идентификации. Мы будем считать, что выбор таких страниц для каждой процедуры записи носит случайный характер и может быть предсказан только с какой-то вероятностью.

Как можно видеть, в такой модели работы памяти для описания процедур записи наиболее удобным и естественным будет использовать аппарат теории вероятности.

Будем рассматривать перезапись i -ой страницы данных как событие, имеющее вероятность P_i^d . Как один из вариантов, величину P_i^d можно определить как отношение числа осуществленных циклов стирания/записи i -ой страницы к числу процедур записи за период эксплуатации SMART-карты. Вероятности P_i^d вместе составляют вектор вероятностей $P^d = (P_0^d, \dots, P_{k-1}^d)$, где k – число страниц данных.

События перезаписи страниц данных не могут быть независимы, так как при каждой процедуре записи перезаписывается хотя бы одна страница данных. Если бы события были независимыми, существовала бы ненулевая вероятность осуществления процедуры записи без реальной записи данных.

Чтобы упростить модель работы с данными в памяти, абстрагируемся от реальной организации работы памяти и допустим возможность осуществления «холостых» процедур записи. В таком случае события перезаписи страниц можно рассматривать как независимые, а вероятность холостой процедуры записи равной $\prod_{i=0}^{k-1} (1 - P_i^d)$.

Для каждой страницы данных с номером i также можно определить зависимые страницы контроля, – те страницы, которые могут измениться в результате перезаписи i -ой страницы данных. Эти зависимости определяются используемым кодом и

характеризуют максимальное количество страниц контроля, которые потребуется перезаписать в результате изменения i -ой страницы данных.

Набор зависимостей между страницами данных и страницами контроля можно описать с помощью матрицы Ω размерности $k \times m$, где $m = N - k$ - число страниц контроля. Элемент Ω_{ij} равен 1 при наличии соответствующей зависимости, и 0 в противном случае. Заметим, что матрица Ω легко строится на основе проверочной матрицы кода H . Матрицу зависимостей Ω можно получить, если убрать из матрицы H^T все строки кроме тех, которые соответствуют контрольным символам кода, и заменить все ненулевые элементы на 1. Например, проверочная матрица H для кода Хемминга $(7, 4)$ имеет вид:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Тогда матрица зависимостей Ω между страницами данных и контроля будет иметь вид:

$$\Omega = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Введем также величины γ_i^d и γ_j^c , где $0 \leq i \leq k - 1$, $0 \leq j \leq m - 1$. Величина γ_i^d будет обозначать число страниц контроля, зависящих от i -ой страницы данных, а γ_j^c будет обозначать число страниц данных, от которых зависит j -ая страница контроля. Следующее утверждение дает ограничение на значения величин γ_i^d и γ_j^c .

Утверждение 1. Если код имеет минимальное расстояние Хемминга d между кодовыми словами, то для любых i таких, что $0 \leq i \leq k - 1$, выполнены неравенства:

$$\gamma_i^d \geq d - 1. \quad (1)$$

Для величин γ_j^c всегда выполнены неравенства:

$$\gamma_1^c \geq 1, \quad (2)$$

$$\sum_{j=0}^{m-1} \gamma_j^c \geq k(d - 1).$$

Доказательство. Вес ненулевых кодовых слов кода с минимальным расстоянием Хемминга d равен d . Это означает что в каждом столбце проверочной матрицы, соответствующем контрольному символу, число ненулевых элементов не менее $d - 1$.

Следовательно, число единиц в любой i -ой строке матрицы зависимостей Ω будет больше или равно $d - 1$. Но это число и есть γ_i^d .

Неравенство (2) очевидно: каждая страница контроля должна зависеть хотя бы одной страницы данных.

Сумма в левой части неравенства, есть не что иное как сумма элементов матрицы Ω . То, что эта сумма больше или равна правой части неравенства, следует из неравенства (1), если применить к нему операцию суммирования по всевозможным i .

Очевидно, что для снижения числа циклов стирания/записи страниц контроля, а тем самым и продления их срока службы, желательным будет иметь код, в котором число зависимостей минимально.

Определим вектор вероятностей $P^c = (P_0^c, \dots, P_{m-1}^c)$ как вектор, элементами которого являются вероятности P_i^c составляющие событие перезаписи хотя бы одной страницы данных во время процедуры записи данных, зависимой от i -ой страницы контроля. События перезаписи страниц контроля в отличие от событий перезаписи страниц данных в общем случае не могут быть рассмотрены как независимые.

Также определим вектор $\tilde{P}^c = (\tilde{P}_0^c, \dots, \tilde{P}_{m-1}^c)$, элементами которого являются вероятности $\tilde{P}_i^c$ перезаписи соответствующих страниц контроля.

Вероятности P_i^c с хорошим приближением оценивают вероятности $\tilde{P}_i^c$, являясь их верхними оценками. Эти вероятности не равны, так как изменение информационных символов кодового слова еще не означает изменение всех его контрольных символов. Связь между векторами P^c и $\tilde{P}^c$ может быть описана с помощью величины δ - условной вероятности того, что при наступлении события изменения зависимых страниц данных, i -ая страница контроля также изменится. Зависимость между P^c и $\tilde{P}^c$ описывается формулой:

$$\tilde{P}^c = \delta P^c.$$

Вероятность δ , как можно показать, зависит только от размера страниц памяти. Действительно, всякий контрольный символ кодового слова может с равной вероятностью принять любое из значений алфавита кодирования. Если мощность алфавита кодирования равна q , а соответствующее число кодовых слов n , то $\delta = 1 - \left(\frac{1}{q}\right)^n$. Но как мощность алфавита кодирования q , так и число кодовых слов n зависят от длины l двоичных последовательностей-символов. Если L — размер страницы памяти в битах, то:

$$q = 2^l,$$

$$n = \frac{L}{l}.$$

Получаем

$$\delta = 1 - \left(\frac{1}{2^l} \right)^{\frac{L}{l}} = 1 - \frac{1}{2^L}.$$

Минимальным размером страницы памяти является один байт, обычными же – 16, 32, 64 байта. Таким образом, в большинстве случаев с большой степенью точности можно считать $\delta \approx 1$.

Векторы P^c и P^d также связаны между собой определенным образом. Для того чтобы описать эту связь, введем следующие обозначения:

$$\ln(v_1, \dots, v_n) \stackrel{\text{def}}{=} (\ln v_1, \dots, \ln v_n),$$

$$\exp(v_1, \dots, v_n) \stackrel{\text{def}}{=} (\exp v_1, \dots, \exp v_n).$$

Также условимся обозначать вектор из единиц размерности n через 1^n . Следующее утверждение дает равенство, связывающее векторы вероятностей P^c и P^d .

Утверждение 2. Пусть код имеет матрицу зависимостей Ω . Тогда для всякого вектора вероятностей P^d справедливо неравенство:

$$\ln(1^m - P^c) = \ln(1^k - P^d) \Omega. \quad (3)$$

Доказательство. Элементы вектора $1^k - P^d$ являются вероятностями того, что соответствующие страницы данных не изменяются при процедуре записи. Аналогично, элементы вектора $1^m - P^c$ являются вероятностями того, что не изменяется ни одна из страниц данных, зависящих от соответствующей страницы контроля. Так как мы считаем события перезаписи страниц данных независимыми, вероятность того, что некоторый набор страниц останется неизменным, равна произведению соответствующих вероятностей $1 - P_i^d$. Иными словами вероятность $1 - P_i^c$ равна произведению вероятностей неизменности зависящих с ней страниц данных.

Для вычисления произведения вероятностей удобно рассматривать вместо них их логарифмы. Благодаря этому произведения вероятностей могут быть заменены на сумму логарифмов вероятностей. Соответствующие суммы логарифмов могут быть записаны в виде равенства (3).

Для изучения зависимости между векторами P^c и P^d полезным является следующее утверждение:

Утверждение 3 Пусть P^d и $\bar{P}^d$ два вектора вероятностей для страниц данных такие, что $P^d \leq \bar{P}^d$. Тогда для соответствующих векторов вероятности P^c и $\bar{P}^c$ для страниц контроля справедливо неравенство $P^c \leq \bar{P}^c$.

Доказательство Матрица зависимостей Ω состоит из единиц и нулей. Поэтому при перемножении с вектором, состоящим из неотрицательных (неположительных) чисел, вновь будет получаться неотрицательный (неположительный) вектор. Векторы $\ln(1^k - \bar{P}^d)$ и $\ln(1^k - P^d)$ являются неположительными. В силу неравенства $P^d \leq \bar{P}^d$ вектор $\bar{P}^d$ может быть представлен как сумма P^d и неотрицательного вектора v :

$$\bar{P}^d = P^d + v.$$

$$\text{Тогда } \ln(1^k - \bar{P}^d) = \ln(1^k - P^d - v) \leq \ln(1^k - P^d).$$

Отсюда получаем, что $\ln(1^k - \bar{P}^d) = \ln(1^k - P^d) + u$, где u - неположительный вектор. Окончательно находим:

$$\ln(1^k - \bar{P}^d)\Omega = \ln(1^k - P^d)\Omega + u\Omega,$$

$$\ln(1^m - \bar{P}^c) = \ln(1^m - P^c) + u\Omega,$$

$$\ln(1^m - \bar{P}^c) \leq \ln(1^m - P^c),$$

$$\bar{P}^c \geq P^c.$$

Сумму элементов вектора вероятностей $\bar{P}^c$ можно интерпретировать как математическое ожидание E_c числа перезаписываемых страниц контроля. Таким же образом определим величину математического ожидания E_d числа записываемых страниц данных:

$$E_c = \sum_{i=0}^{m-1} \bar{P}_i^c = \delta \sum_{i=0}^{m-1} P_i^c,$$

$$E_d = \sum_{i=0}^{k-1} P_i^d.$$

Заметим, что величина E_d всегда должна быть больше или равна 1, что накладывает определенные ограничения на вектор вероятностей P^d . В силу замечаний выше, для любого кода, исправляющего не менее одной ошибки, величина E_c при этом будет не меньше 2.

Определим для помехоустойчивого кода, задаваемого на страницах памяти, функцию $R(P^d)$ от вектора вероятности P^d :

$$R(P^d) \stackrel{\text{def}}{=} \frac{E_c(P^d)}{E_d(P^d)}.$$

Поведение функции $R(P^d)$ во многом описывает эффективность исследуемого кода в плане использования части памяти для контрольных данных. Чем меньшие значения принимает функция, тем более эффективным является код.

Другим важным показателем эффективности кода является векторная величина

$$\rho = (\rho_0, \dots, \rho_{m-1}) = \frac{1}{\max P_j^d} \tilde{P}^c.$$

Эта величина характеризует то, насколько чаще происходит перезапись каждой страницы контроля, чем самой нагруженной страницы данных. Параметр ρ является очень важным показателем. Так как число циклов стирания/записи страниц памяти ЭСППЗУ ограничено, рано или поздно происходит их выход из строя, и величина ρ может охарактеризовать число испорченных страниц контроля до первого выхода из строя страницы данных. При достижении гарантийного значения числа циклов стирания/записи для i -ой страницы контроля число циклов перезаписи для страниц данных будет не более $1/\rho_i$. Если считать, что при достижении гарантийного числа циклов стирания/записи страница памяти выходит из строя, то в действительности число страниц памяти, необходимых для хранения контрольной информации, равно сумме величин ρ_i , округленных да большего целого. Обозначим эту величину $\tilde{m}$ и приведем формулу для ее вычисления:

$$\tilde{m} = -\sum_{i=0}^{m-1} [-\rho_i].$$

Определим относительный расход памяти ε и действительный относительный расход памяти $\tilde{\varepsilon}$:

$$\varepsilon = \frac{m}{k},$$

$$\tilde{\varepsilon} = \frac{\tilde{m}}{k}.$$

Величины ε и $\tilde{\varepsilon}$ могут показывать границы применимости кода для рассматриваемого случая. При этом величина $\tilde{\varepsilon}$ является функцией $\tilde{\varepsilon}$ от вектора вероятностей P^d и показывает действительный объем памяти необходимый для работы кода до обнаружения первого сбоя страницы данных.

Модель последовательного выбора страниц памяти для записи

Рассмотрим ситуацию использования памяти ЭСППЗУ, когда перезапись страниц данных не происходит (или происходит редко), а имеет место только запись новых данных в свободные страницы памяти.

Для такой модели использования памяти число циклов стирания/записи страниц данных фактически не возрастает, и потому на протяжении всего периода эксплуатации остается незначительным по сравнению с гарантийным числом циклов стирания/записи.

В такой ситуации выход из строя страниц памяти возникает с наибольшей вероятностью либо в результате внешних воздействий (электромагнитные помехи, высокая температура и др.), либо при приближающемся сроке окончания службы устройства. А потому более вероятными становятся выходы из строя сразу нескольких страниц памяти. Таким образом, большее значение приобретают коды, исправляющие более одной ошибки.

Число циклов стирания/записи страниц контроля в отличие от страниц данных будет возрастать по мере добавления в память новых данных, и можно предположить, что будет возрастать пропорционально количеству данных. Если число процедур записи достаточно большое, то вероятность выхода из строя страниц контроля становится значительно больше, чем для страниц данных.

С чрезмерным увеличением числа циклов перезаписи страниц контроля можно справиться, если разбить массив страниц данных на несколько частей, и каждый полученный набор страниц кодировать отдельно. При этом защищенность от многократных потерь страниц данных возрастет, но вместе с ней возрастет и число необходимых страниц контроля.

В частности, можно использовать коды, исправляющие одну ошибку, применяя их к небольшим массивам страниц данных. При этом не будут корректироваться сбои сразу двух страниц данных в одном подмассиве. Поэтому такой вариант кодирования является менее надежным, чем кодирование целиком всех страниц данных кодом, исправляющим несколько ошибок. Положительным же эффектом разбиения массива страниц данных на части будет уменьшение нагрузки на страницы контроля. Выбор того, разбивать или нет массив страниц данных на несколько подмассивов, зависит от конкретной ситуации и используемого кода.

Заключение

В статье рассмотрены модели систем обеспечивающих идентификацию, и проведен анализ моделей случайной и последовательной выборки данных из ЭСППЗУ. По итогам

изучения моделей определены показатели, оценивающие алгоритмы, повышающие надежность функционирования персональных систем идентификации. Эффективность кода характеризует то, насколько часто происходит перезапись каждой страницы контроля, чем самой нагруженной страницы данных. Относительный и действительный расход памяти для определения объема памяти, необходимого для работы кода до обнаружения первого сбоя страницы данных. С помощью данных показателей могут быть оценены алгоритмы помехоустойчивого кодирования для персональных устройств идентификации.

Список литературы

1. Wolfgang R., Wolfgang E. Smart Card Handbook. John Wiley & Sons, 2011. 1025 p.
2. Лахири С. RFID. Руководство по внедрению. М.: Кудиц-Пресс, 2007. 312 с. [Lahiri S. The RFID Sourcebook. IBM Press, 2005. 304 p.].
3. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. 576 с. [Blahut R. Theory and Practice of Error Control Codes. Addison-Wesley, Reading, 1983. 500 p.].

Action models of personal identification systems with antinoise coding procedures

10, October 2012

DOI: 10.7463/1012.0486630

Kryukov D.A.

Russia, Moscow State Technical University MIREA

dm.bk@bk.ru

The article considers models of systems ensuring identification; it gives an analysis of models of random and sequential retrieval from electronically erasable programmable read-only memory. On the basis of the obtained models the author defines mathematical criteria for evaluating the degree of effectiveness of antinoise coding and storage requirements. In the process of proving the allegations in the probabilistic evaluation it is suggested that the Hamming code be used.

Publications with keywords: [SMART-card](#), [ID-systems](#), [Hamming code](#), [ECC](#), [error-correcting coding efficiency](#), [discharge memory coefficient](#)

Publications with words: [SMART-card](#), [ID-systems](#), [Hamming code](#), [ECC](#), [error-correcting coding efficiency](#), [discharge memory coefficient](#)

References

1. Wolfgang R., Wolfgang E. *Smart Card Handbook*. John Wiley & Sons, 2011. 1025 p.
2. Lahiri S. *The RFID Sourcebook*. IBM Press, 2005. 304 p. (Russ. ed.: Lakhiri S. *RFID. Rukovodstvo po vnedreniiu*. Moscow, Kudits-Press, 2007. 312 p.).
3. Blahut R. *Theory and Practice of Error Control Codes*. Addison-Wesley, Reading, 1983. 500 p. (Russ. ed.: Bleikhut R. *Teoriia i praktika kodov, kontroliruiushchikh oshibki*. Moscow, Mir, 1986. 576 p.).