УДК 519.7 DOI 10.17223/2226308X/11/32

О КОДАХ, ИСПОЛЬЗУЮЩИХСЯ В БИОМЕТРИЧЕСКИХ КРИПТОСИСТЕМАХ[1]

А. А. Белоусова, В. И. Нобелева, Н. Н. Токарева

Рассмотрены вопросы использования кодов, исправляющих ошибки, в биометрических криптосистемах. Предложены конструкции кодов, имеющих параметры лучше, чем у кода, используемого F. Hao, R. Anderson, J. Daugman (2006) в оригинальной биометрической криптосистеме. Предложена новая верхняя оценка мощности кода, учитывающая не только кодовое расстояние $d = 2t+1$, но и ненулевую вероятность исправления кодом $t+1$ ошибки; в случае $t = 0, 1, 2$ исследованы возможности достижения новой границы.

Ключевые слова: *биометрическая криптосистема, линейный код, верхняя оценка.*

Использование биометрических данных в криптографических целях в настоящее время очень актуально. Радужная оболочка глаза служит одной из самых надёжных биометрических характеристик человека. Существуют методы, позволяющие выделить по ней 2048 битов информации, однозначно идентифицирующих человека, — так называемый биометрический код. При этом известно, что два таких кода при различных измерениях у одного человека отличаются не более чем на 10–20 %, а у разных людей — не менее чем на 40–60 %. С помощью биометрического кода можно не только проводить аутентификацию (идентификацию личности с последующей проверкой), но и защищать секретную информацию, маскируя её с помощью кода и сохраняя на смарт-карте. Воспользоваться секретной информацией с карты (биометрическим ключом) сможет только тот абонент, чей биометрический код окажется правильным. При этом система не хранит биометрические данные пользователей, а проверка осуществляется в процессе выполнения специального криптографического протокола [1].

Согласно протоколу, дважды происходит сложение ключа с биометрическим кодом пользователя — до записи на смарт-карту и при чтении информации с неё. Учитывая, что при этом в биометрический ключ могут быть внесены до 10–20 % ошибок, необходимо использовать помехоустойчивое кодирование для восстановления правильного ключа. Для этой цели в оригинальной работе [1] используется прямое произведение кода Адамара с параметрами [64,7,32] и кода Рида — Соломона [32,20,13] над $\mathrm{GF}(2^7)$. Однако до конца не ясно, насколько эффективным является использование именно этого кода.

В данной работе предложена конструкция помехоустойчивого кода, имеющего параметры лучше, чем у кода из [1] (это код длины $n = 2048$, размерности $k = 140$, с кодовым расстоянием $d = 416$), а именно: предложен LDPC-код длины $n = 2048$, размерности $k = 517$. Экспериментально проверено, что с погрешностью 5 % новый код исправляет до 20 % ошибок при передаче информации.

В работе также рассмотрена возникающая здесь новая задача в области теории кодирования. С одной стороны, использующийся в биометрической криптосистеме код должен иметь достаточно большое кодовое расстояние $d = 2t+1$, а значит, с гарантией корректировать достаточно большое число ошибок, равное t. С другой стороны, его

[1]Работа выполнена при финансовой поддержке РФФИ (проекты № 17-41-543364, 18-07-01394), Министерства образования и науки (задание № 1.12875.2018/12.1 и Программа 5-100), Программы фундаментальных научных исследований СО РАН № I.5.1., проект № 0314-2016-0017.

корректирующие способности в среднем не должны быть слишком высокими, чтобы в большинстве случаев при декодировании не допустить исправления больше чем $t+s$ ошибок. Рассмотрены теоретические возможности создания таких кодов. В частности, сделан первый шаг к выделению более сложной оценки мощности кода, учитывающей не только кодовое расстояние $d = 2t + 1$, но и ненулевую вероятность исправления кодом $t + 1$ ошибки.

Пусть C — двоичный (n, d)-код; $A(x) = \{y \in \mathbb{F}_2^n : \mathrm{d}(x, y) \leqslant \min\limits_{z \in C, z \neq x} \mathrm{d}(z, y)\}$ — множество векторов булева куба, для которых x является ближайшим кодовым вектором; при каждом x определены множества $B(x) \subseteq A(x)$ таким образом, что для любых различных x, x' множества $B(x)$ и $B(x')$ не пересекаются и выполняется $\bigcup\limits_{x \in C} B(x) = \mathbb{F}_2^n$.

Теорема 1. Пусть для любого кодового слова x двоичного (n, d)-кода C выполняется $|B(x)| \leqslant \ell$. Тогда $|C| \leqslant 2^n/\ell$.

Теорема 2. Если $n = 2^m - 1$, $\ell = n + 1$, то оценка теоремы 1 достигается на совершенных кодах. Если $n = 2^m - 1$, m чётно, $\ell = 1 + n + \mathrm{C}_n^2 + n(n + 3)/2$, то оценка теоремы 1 достигается на кодах Препараты.

ЛИТЕРАТУРА

1. *Hao F., Anderson R., and Daugman J.* Combining Crypto with biometrics effectively // IEEE Trans. Comput. 2006. V. 55. No. 9. P. 1081–1088.

УДК 519.1 DOI 10.17223/2226308X/11/33

О КОЛИЧЕСТВЕ АТТРАКТОРОВ В КОНЕЧНЫХ ДИНАМИЧЕСКИХ СИСТЕМАХ ОРИЕНТАЦИЙ ПОЛНЫХ ГРАФОВ

А. В. Жаркова

Рассматриваются конечные динамические системы ориентаций полных графов. Состояниями системы являются все возможные ориентации полного графа, а эволюционная функция задаётся так: динамическим образом орграфа является орграф, полученный из исходного путём переориентации всех дуг, входящих в стоки, других отличий между исходным орграфом и его образом нет. Подсчитывается количество аттракторов в системе, приводятся соответствующие таблицы для конечных динамических систем ориентаций полных графов с количеством вершин от двух до десяти включительно.

Ключевые слова: *аттрактор, граф, конечная динамическая система, ориентация графа, полный граф, турнир, эволюционная функция.*

Графовые модели, в которых отказы процессоров интерпретируются как удаление соответствующих вершин, а отказы сетевых каналов — как удаление дуг, занимают важное место в задачах, связанных с отказоустойчивостью компьютерных сетей. При изучении модельных графов можно применять идеи и методы теории конечных динамических систем, в частности динамических систем двоичных векторов [1, 2], — когда имеется естественная двоичная кодировка графов рассматриваемого класса. В модели [3] в качестве механизма восстановления работоспособности сети предлагается так называемая SER-динамика бесконтурных связных ориентированных графов. В настоящей работе полные графы изучаются с точки зрения динамического подхода к отказоустойчивости графовых систем.