УДК 004.056

В.Ю. Королев, В.В. Полиновский

Комбинаторная модель украинского ключа–аутентификатора и считывателя

Описаны варианты конструкции украинского ключа-аутентификатора и общая методика расчета количества комбинаций и длины кода. Построена комбинаторная модель ключа и считывателя. Показано, что система УАК-считыватель позволяет получить длину кода, соответствующую криптографическим стандартам.

The descriptions of the Ukrainian-authenticator key (UAK) design options are given. The Constructions of the combinatorial model key and reader are discussed. A general method for calculating the number of combinations and the length of the code is presented. It was shown, that the system UAK-reader gives the code length corresponding to cryptographic standards.

Описано варіанти конструкції українського ключа–автентифікатора. Побудовано комбінаторну модель ключа та зчитувача. Представлено загальну методику розрахунку кількості комбінацій і довжин коду. Показано, що система УАК-зчитувач дозволяє отримати довжину коду, яка відповідає криптографічним стандартам.

Введение. В современных информационных системах данные в основном хранятся и передаются в электронном виде. Однако все преимущества компьютеризированных систем связи и хранения данных возможны, если обеспечена безопасность доступа, хранения и передачи информации. Сегодня почти все корпоративные и частные информационные системы работают с использованием тех или иных средств аутентификации пользователей, в то же время, в СМИ постоянно публикуют сообщения о взломе и краже как корпоративных, так и персональных данных. Поэтому надежность компьютерной безопасности в перечне требований к информационным системам занимает первые позиции. Частые случаи несанкционированного доступа связаны с несовершенством средств аутентификации и протоколов передачи данных [1–8]. Следовательно, современные сложные информационные и технические системы нуждаются в постоянном совершенствовании средств аутентификации пользователей с надежной системой передачи информации с ограниченным доступом.

Украинский ключ–аутентификатор представляет собой механический носитель кодовой информации, который используется со считывателями этой информации и служит способом идентификации и аутентификации для устройств, с помощью которых определяется право доступа к любым объектам и системам [1].

К таким способам и устройствам выдвигаются следующие требования:

- надежная защита объектов от несанкционированного доступа;
- надежная и простая конструкция;
- надежный и простой способ применения, понятный обычному пользователю любого возраста и уровня подготовки.

Постановка задачи

Известен ряд механических аналогов по определенным показателям предложенной конструкции [2]. Однако их общий недостаток – малая комбинаторная емкость для использования в современных системах защиты информации. Задача авторов – построение комбинаторной модели ключа и считывателя с целью обоснования того, что предложенный аутентификатор соответствует современным требованиям к длине ключа, принятым в системах защиты информации.

Основная часть

В статье предложен отечественный механический ключ–аутентификатор (УАК), ключевое пространство которого составляет порядка 2^{192} комбинаций (при использовании стандартной комплектации) или более. По своим характеристикам этот ключ уникален не только в Украине, но в мире. Рассмотрим принципы его работы.

Ключ состоит из объемных секретных элементов – пластин (рис. 1), которые могут иметь

любую форму и содержат кодовые отверстия, фиксаторы и кодовые символы, помогающих пользователю запоминать выбранный код в цифробуквенном (символьном) виде. Весь набор пластин подпружинен вдоль оси стержня. Это дает возможность вручную изменять кодовую последовательность и значительно облегчает процесс набора и запоминания комбинации. Кроме этого, такое разнообразие форм позволяет на порядки увеличить количество комбинаций ключа.

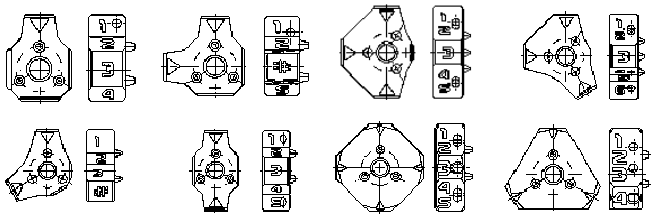


Рис. 1. Секретные элементы ключа разных форм

Такое построение дает следующие преимущества:

1. *Кодовые каналы*. В отличие от своего предшественника [2], ключ–аутентификатор имеет объемные секретные элементы, в которых может быть несколько кодовых каналов (рис. 2). С их помощью происходит считывание кодовой комбинации и последующая генерация пароля.

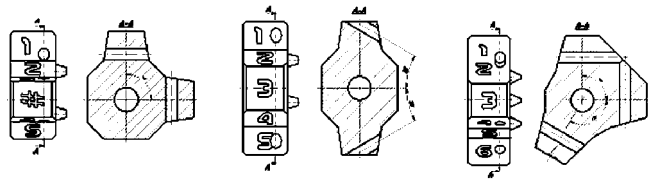


Рис. 2. Варианты размещения кодовых каналов элемента

2. *Возможность перекрытия отдельных отверстий*. На некоторых секретных элементах есть специальные винты, с помощью которых можно перекрывать определенные каналы (рис. 3). Благодаря этому значительно расширяется количество возможных кодовых комбинаций и, как будет показано, использование перекрываемых кодовых каналов позволяет решить проблему снижения количества комбинаций для симметричных пластин. Для анизотропного распространения света в кодовых каналах, в зависимости от длины волны светодиода передатчика, например, может быть использована технология внедрения в канал материалов с нелинейными оптическими характеристиками.

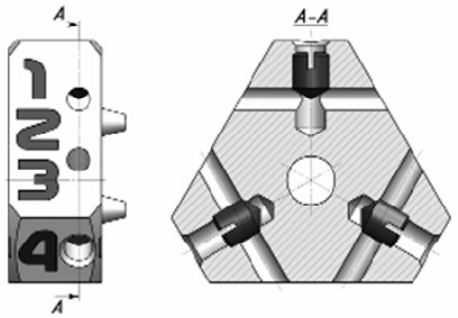


Рис. 3. Возможность перекрытия каналов элемента

3. *Фиксаторы и кодовые символы*. На каждом секретном элементе ключа есть специальные выступы–фиксаторы и кодовые символы. Они позволяют фиксировать угол секретного элемента при повороте относительно других элементов. На каждую грань элемента (полюс) нанесены символы, которые позволяют безошибочно устанавливать нужный код.

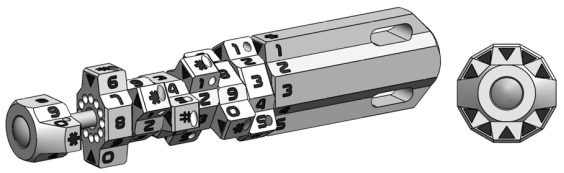


Рис. 4. Вращение секретных элементов ключа–аутентификатора вокруг оси

4. *Разнообразие форм*. Форма элементов может быть разной: треугольник, четырехугольник, пятиугольник и другие многогранники разного вида в том числе асимметричные.

а *б*

Рис. 5. Аутентификатор, состоящий из: *а* – двухполюсных и *б* – трехполюсных секретных элементов

5. *Выбор количества элементов и формы*. Пользователь по собственному желанию может решать, сколько секретных элементов будет содержать ключ и в каком порядке они будут размещены, какой формы будут эти элементы, количество и угол кодовых отверстий. Он также может самостоятельно определять, следует ли ему перекрывать кодовые отверстия винтами (формируя, например долговременный ключ) или нет. При этом каждый ключ

становится уникальным и имеет собственный набор кодовых комбинаций.

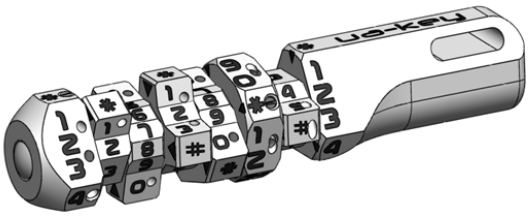


Рис. 6. Аутентификатор, состоящий из разных по форме секретных элементов

6. *При краже ключа* злоумышленник не получит доступ к паролям пользователя, поскольку только пользователь знает правильное положение секретных элементов, а подобрать код перебором за приемлемое время почти невозможно.

7. *Универсальность применения ключа*. Пользователь без каких-либо специальных устройств может вручную быстро изменять общее количество, последовательность и положение секретных элементов. Так, с помощью одного ключа можно задать множество различных паролей и работать с неограниченным количеством устройств, которые имеют встроенный считыватель кодовой комбинации (мышь для работы с компьютером, сейф, дверной замок и др.).

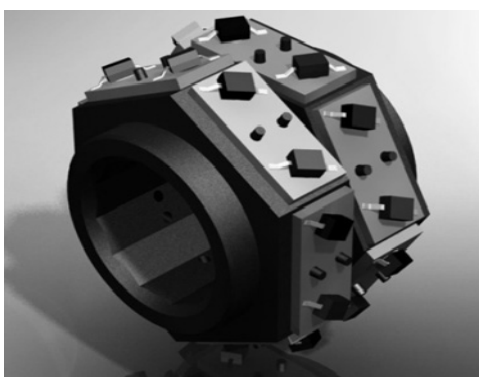


Рис. 7. Унифицированный считыватель на 12 пластин может считывать сложные комбинации ключа с разным набором сегментов

8. *Унифицированный считыватель УАК*. В настоящее время разработаны два уникальных устройства считывания для всех возможных ключей УАК (имеющих разную длину, сегменты неодинаковой формы и типа с разными углами размещения секретных каналов). При прохождении УАК через скважину начинается работа контрольного устройства (считывателя информации).

Конструкция считывателя была усовершенствована так, чтобы считыватель ключа–аутентификатора мог состоять из произвольной минимального необходимого количества считывающих элементов, считывать разные виды ключей–аутентификаторов, иметь несколько степеней считывания и свойство простого монтажа.

Комбинаторная модель УАК

Каждая пластина УАК в общем случае представляет собой многогранник (составную прямоугольную призму). Считывание информационных признаков с пластин УАК заключается в регистрации основания многоугольника (переднего края формы многогранника); количества и пространственного расположения отверстий; тыльной части (края) формы. Соответственно, имеем три группы считанных сигналов от оптопар: две группы фиксируют основание многогранника и одна – отверстия в ней. Чтобы описать процесс получения секретного кода при последовательном изменении откликов от оптопар по мере продвижения многогранника внутри шахты введем понятие информативного сечения (ИС). ИС – это упорядоченная информация, которую получают при считывании формы пластины УАК или расположения отверстий на гранях УАК, количество которых равно числу оптопар. На рис. 8 показано соответствие между считанной информацией и пластиной УАК. Видно, что минимальное количество информационных сечений равно трем, хотя может быть дополнено до любого количества, эксплуатационно рационального.

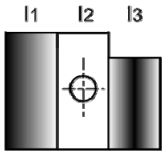


Рис. 8. Эскиз полюса пластины УАК (вид сверху). I_1, I_2, I_3 – информационные сечения

Рассчитаем количество комбинаций для форм пластин УАК (информационные срезы I_1, I_3). Очевидно, что количество комбинаций для формы определяется количеством уникальных сигнальных откликов от оптопар, причем для симметричных пластин количество комбинаций уменьшается пропорционально числу симмет-

ричных полюсов относительно центра. Следовательно, имеем формулу:

$$V_c = \sum_{i=1}^{Z} C_i \times \frac{P_i}{S_i},$$

где G_i – количество пластин с определенным числом полюсов, P_i – количество сторон многоугольника считывателя, S_i – количество симметричных полюсов у пластины в фронтальной плоскости, Z – общее количество пластин всех видов.

Количество вариантов полюсов пластины

Количество полюсов может варьироваться от единицы до N. Соответственно, количество комбинаций перекрытых лучей будет определяться сочетаниями полюсов, так как для расчета возможного числа деталей порядок их расстановок не имеет значения [9]:

$$C^0_N + C^1_N + \ldots + C^N_N = 2^N.$$

Полюс также может варьироваться по ширине (рис. 9 и 10). На рис. 9 показаны шесть возможных вариантов ширины полюса пластины (кроме основного, седьмого – по всей ширине).

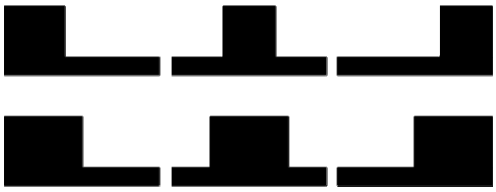


Рис. 9. Вариации ширины полюса для пластины УАК

Максимальное количество вариантов ширины полюса определяется механической устойчивостью конструкции и разрешающей способностью сетки лучей оптопар, т.е. полюс должен пересекать (частично затенять) хотя бы один луч (рис. 10).

Рассчитаем количество комбинаций для вариаций ширины полюса пластины УАК. Если объект A можно выбрать m способами и если после каждого такого выбора объект B можно выбрать n способами, то выбор пары (A, B) в указанном порядке можно осуществить $n \times m$ способами. Пусть Z – число конструкционных вариантов ширины полюса, тогда 2^{NZ} – количество комбинаций формы для всех вариантов полюсов. Для 12 граней ридера и семи вариантов полюса имеем 2^{84}, для 10 граней и семи вариантов полюса имеем 2^{70} (вариантов для одной пластины). Таким образом, для M пластин имеем 2^{NZM} – комбинаций.

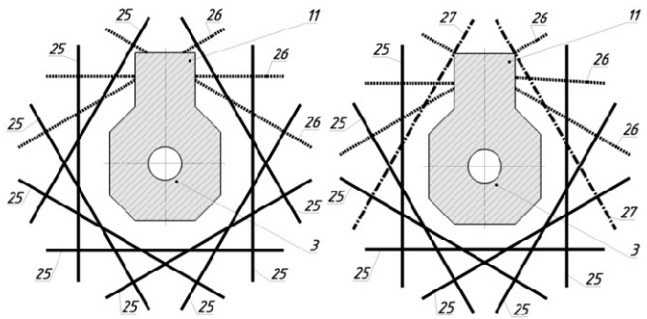


Рис. 10. Вариации количества считанных откликов оптопар от ширины полюса

Таблица 1. Количество комбинаций для форм УАК пластин (показатель степени 2)

Количество пластин	Количество граней считывателя	
	X	XII
8	560	672
14	980	1176

Общее количество вариантов исполнения пластины определяется числом вариантов разбиения основания составной призмы (выпуклого 10-ти- или 12-тиугольника) на геометрические фигуры (выпуклые и вогнутые многоугольники), которые можно вписать в считыватель. Очевидно, что такая задача требует отдельной формализации и декомпозиции, поэтому приведем оценку снизу количества фигур. Для этого используем определение количества вписанных треугольников в многоугольник. Количество разбиений выпуклого (n+2)-угольника на треугольники непересекающимися диагоналями составит [9]: $K_n = \frac{1}{n+1} \times C^n_{2n}$, где n – количество вершин, K_n – числа Каталана. Для 10-ти- и 12-тиугольников имеем: $K_{10} = 16796 \approx 2^{14}$, $K_{12} = 208012 \approx 2^{18}$.

С точки зрения комбинаторики [9] задачу поиска максимума комбинаций на сетке лучей можно представить как размещения (расстановки), перестановки или сочетания групп из k-предметов из n. Выбор модели определяется процессом считывания и конструкцией пластин ключа. Максимально возможное количество комбинаций определяется n-расстановками из n раз-

личных предметов и для 12-ти оптопар составляет $n^n = 12^{12} \approx 2^{43}$. В настоящее время реализован способ регистрации отверстий и форм основания пластин без учета порядка их считывания, описываемый суммой сочетаний. Дальнейшее развитие предполагает создание новой конструкции ключа и считывателя, позволяющего учитывать порядок взаимодействия лучей с конфигурацией ключа. Такая модель работы системы ключ–считыватель описывается перестановками, и поскольку $A_n^k = n! C_n^k$, то количество комбинаций возрастет в $n!$ раз. Для 12-ти оптопар количество комбинаций увеличится приблизительно в 10^{20} раз, до 2^{41} для одной пластины.

Расчет количества комбинаций для отверстий в пластинах УАК

Исходя из принципа работы считывателя и ключа можно сделать вывод, что последовательность регистрации оптопарами отверстий информационного среза в пластине несущественна, а важно только их количество и размещение на гранях. Такой постановке задачи соответствуют сочетания в комбинаторике, т.е. интерес представляет не порядок элементов в комбинациях, а их состав. Воспользуемся следующим определением для сочетаний: *k*-сочетаниями из *n*-элементов называют все возможные *k*-расстановки, составленные из этих элементов и отличающиеся одна от другой составом, а не порядком элементов. Следовательно, количество комбинаций отверстий в пластинах УАК, зарегистрированных оптопарами определяется соотношением

$$C_N^k = \frac{N!}{(N-k)!k!},$$

где k – количество оптопар в пластине УАК, N – общее количество оптопар.

Определим *максимальное количество комбинаций для информационного слоя отверстий УАК.* Для ключа из M пластин количество комбинаций определяется следующим произведением: $\prod_{i=1}^{M} C_N^{k_i}$, где k_i – количество активных оптопар для пластины. Известно, что функция сочетаний C_N^k подобна перевернутой параболе, симметрична и имеет один максимум в точке $N/2$. Поэтому максимальное количество комбинаций для ключа будет в том случае, когда количество откликов от отверстий на всех пластинах будет $k = N/2$. При этом максимальное количество комбинаций для ключа из M-пластин равно: $\left(C_N^{N/2}\right)^M = \left(\frac{N!}{\left[\frac{N}{2}!\right]^2}\right)^M$.

Минимальное количество комбинаций, равное единице, дают вырожденные конфигурации пластин – без отверстий или с количеством отверстий, равным числу пластин M. Эксплуатационно рациональному минимальному количеству комбинаций соответствует пластина с одним отверстием или пластина с количеством отверстий, равным $N - 1$. В обоих случаях количество комбинаций для УАК из M пластин равно N^M.

Рассчитаем количество комбинаций, которое может ввести в считыватель пластина различной формы с информационного слоя отверстий. При введении одной пластины в считыватель количество комбинаций соответствует сумме сочетаний для всех конфигураций отверстий для пластины. Воспользовавшись известным в комбинаторике соотношением, получим:

$$C^0_N + C^1_N + C^2_N + \ldots + C^{N-1}_N + C^N_N = 2^N.$$

Методика расчета количества комбинаций для ключа и считывателя

С целью расчета количества комбинаций кодирующую конструкцию многогранника УАК можно разделить на форму пластины и отверстия в форме (кодовые каналы). Выбор такого разделения обусловлен стадиями процесса изменения конфигурации светового поля внутри считывателя по мере прохождения пластин УАК вдоль шахты. Действительно, сначала состояние светового поля изменяется только формой пластин (многогранников) (этап 1 – информационное сечение I_1), а затем, по мере движения ключа в глубину шахты, через отверстия в пластине проходят лучи (этап 2 – информационное сечение I_2) и, в конце процесса, регистрируется инфор-

мационное сечение I_3, соответствующее тылу формы. В настоящее время, конфигурация пластин ключа такова, что $I_1 = I_3$. Поэтому, в результате регистрации процесса прохождения пластины вдоль считывателя УАК имеем два состояния для элемента УАК: затемнение лучей формой и регистрация лучей, проходящих сквозь отверстия в пластине. Таким образом, при регистрации кода с пластины УАК получаем одну кодовую комбинацию от формы пластины–многогранника и одну кодовую комбинацию от пластины с отверстиями. Для считывателя – форма ключа дает количество (симметричных) поворотов, а перфорированная пластина дает сочетание комбинаций. Поскольку это два различных класса комбинаций и каждая комбинация входит только в один класс, то общее количество комбинаций для пластины подчиняется правилу суммы комбинаций: если некоторый объект A можно выбрать m способами, а объект B можно выбрать n способами, то выбор либо A, либо B можно осуществить $m + n$ способами.

Для вариантов конструкции пластин, которые представляют собой несколько последовательных соосных рядов с отверстиями в разных формах, выполненных как одна монолитная деталь (составной многогранник), расчет количества комбинаций сводится к вычислению количества комбинаций для каждой элементарной пластины (табл. 2).

Определение количества комбинаций для ключа и считывателя

1. В конструкции составного сегмента можно выделить простые структуры (элементарные многогранники: форма пластины и пластина с отверстиями «перфорированная форма»). Если многогранник несоставной см. п. 2.

2. Для простого многогранника ключа форма пластины создает одну группу комбинаций, а для перфорированной формы – одно сочетание комбинаций. Для считывателя – форма ключа дает количество (симметричных) поворотов, а перфорированная пластина дает сочетание комбинаций.

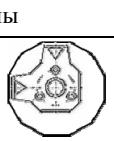
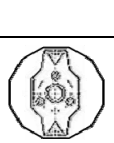
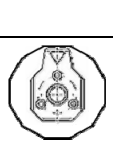
3. Общее количество кодовых комбинаций для ключа описывается правилом произведения комбинаций от пластин: если объект A можно выбрать m способами и если после каждого такого выбора объект B можно выбрать n способами, то выбор пары (A, B) в указанном порядке можно осуществить $m \times n$ способами, т.е. количество комбинаций для ключа – это произведение всех кодовых комбинаций от перфорированных пластин и форм пластин. Поскольку форма пластины и пластины с отверстиями – единая конструкционная (сборная) единица – деталь и вместе они дают независимые кодовые комбинации соответственно, то количество кодовых комбинаций суммируется, а не перемножается, как в случае отдельных ИС:

$$UAK = \prod_{i=1}^{M} \left(C_N^{k_i} + q_i \right),$$

где C^{ki}_N – количество комбинаций, задаваемое отверстиями конкретного (установленного) i-го сегмента, q_i – количество поворотов сегмента с отверстиями, дающими уникальные кодовые комбинации (табл. 2). Количество уникальных комбинаций сокращается в число раз от количества симметричных относительно центра полюсов пластины. Из табл. 2 видно также (форма 4), что добавление ассиметричного полюса к симметричным приводит к увеличению количества комбинаций. Также решением проблемы уменьшения количества комбинаций для симметричных пластин есть выполнение в них пропилов (рис. 2 и 3), которыми варьируют выходной код ИС.

Обще количество кодовых комбинаций считывателя ключа (полное количество всех кодовых состояний системы) – это сумма всех ком-

Таблица 2. Количество комбинаций для пластин УАК различной формы

Количество								
Симметр. полюсов	4	3	–	1	–	2	–	–
Комбинаций	3	4	12	12	12	6	12	12

бинаций для формы сегмента и сумма всех сочетаний для пластин, т.е.:

$$R = \left[\sum_{i=1}^{N} \left(C_N^{k_i} + \bar{q}_i \right) \right]^M = \left[2^N + \sum_{i=1}^{N} \bar{q}_i \right]^M \approx 2^{N-M}.$$

$$C_N^{N_{\text{Star}}} + \ldots + C_N^{N-1} + C_N^N = 2^N - \left(C_N^0 + C_N^1 + \ldots + C_N^{N_{\text{Star}}-1} \right).$$

$$R = \left[\sum_{i=1}^{N} \left(C_N^{k_i} + C_N^{q_i} \right) \right]^M = \left[2^{N+1} - \sum_{i=1}^{N_{\text{Star}}-1} C_N^{q_i} \right]^M \approx 2^{N-M}.$$

M – количество сегментов, N – количество оптопар, k_i – количество лучей, q_i – количество поворотов, задающих независимые комбинации для форм сегментов, $C_N^{g_i}$ – количество комбинаций для пропущенных формой лучей, N_{Start} – минимальное количество лучей, перекрываемых формой с одной особенностью, g_i – количество лучей, перекрываемых формой, причем их меньше, чем N_{Start}, $C_N^{g_i}$ – количество виртуальных комбинаций для задержанных (затемненных, прерванных, перекрытых) формой лучей. Таким образом, количество комбинаций, которые дают отверстия в пластинах будет значительно больше, чем количество комбинаций, которые дают формы многогранника.

Следовательно, для системы считыватель – УАК для ключа, состоящего из M пластин, количество комбинаций составляет 2^{MN}. Поскольку результат считывания описывается состоянием 10–12 оптопар, то длинна выходного кода считывателя в битах равна произведению количества комбинаций на число оптопар. Сведем полученные результаты в табл. 3, где приведено приближенное до степени 2 количество комбинаций и длинна кода для УАК и считывателя при 10/X и 12/XII оптопарах (N) для одного (для двух введений) и для 8 и 14 пластин (M).

Таким образом, количество комбинаций и длина выходного кода для УАК-системы превосходит требования современных криптографических стандартов защиты информации, которые рекомендуют длины ключей аутентификации 256 бит.

Заключение. Предложенный отечественный механический ключ–аутентификатор по своим характеристикам уникален, эффективен и универсален. Следует отметить, что положителен и тот факт, что считывание всех возможных вариантов УАК ключами разной длины с пластинами неодинаковой формы и типа, с различными углами размещения секретных элементов, можно регистрировать одним универсальным считывателем.

Комбинаторный анализ отечественного механического ключа–аутентификатора показывает, что количество комбинаций для УАК-системы превосходит требования криптографических стандартов защиты информации, которые рекомендуют длины ключей аутентификации 128–256 бит.

Предложенная комбинаторная модель позволяет строить различные системы персонализации и защиты информации и технических систем в зависимости от задач и стоимости эксплуатации.

Все это позволяет создавать современные универсальные системы аутентификации пользователей с повышенным уровнем защиты секретной информации.

Дальнейшее развитие предполагает создание новой конструкции ключа и считывателя, позволяющего учитывать порядок взаимодействия лучей с конфигурацией ключа. Такая модель работы системы ключ–считыватель позволит увеличить количество комбинаций приблизительно в 10^{20} раз.

Таблица 3. Количество комбинаций и длинна кода для УАК и считывателя

Количество пластин УАК	Максимум считывателя				Максимум ключа				Рациональный минимум считывателя и ключа			
	X		XII		X		XII		X		XII	
8	2^{80}	800	2^{96}	1153	2^{64}	640	2^{79}	951	2^{27}	270	2^{29}	545
	2^{160}	1600	2^{192}	2307	2^{128}	1280	2^{158}	1930	2^{53}	530	2^{57}	1089
14	2^{140}	1400	2^{168}	2218	2^{112}	1120	2^{138}	1665	2^{46}	460	2^{50}	953
	2^{280}	2800	2^{336}	4037	2^{223}	2230	2^{276}	3302	2^{93}	930	2^{100}	1906

Окончание на стр. 80

1. *Пат*. UA 89745 Україна, МПК (2009) E 05B 19/00 Спосіб автентифікації і введення кодової інформації та автентифікат зі зчитувачем кодової інформації для його здійснення / В.В. Поліновський, О.М. Ходзінський та ін. // Заявл. 06.08.2009; Опубл. 25.02.2010, Бюл. № 4.
2. *Бардаченко В.Ф.*, *Корольов В.Ю.* Концепция построения систем персонализации на базе расширения вектора кодов ВІК-ключа // УСиМ. – 2007. – № 1. – С. 53–61.
3. *Королев В.Ю.*, *Полиновский В.В.*, *Герасименко В.А.* Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей // Там же. – 2011. – № 1. – С. 79–87.
4. *Персонализация* мобильных телекоммуникационных и вычислительных средств методом оптической регистрации ВІК-кода / В.Ф. Бардаченко, В.Ю. Королев, В.В. Полиновский и др. // УСиМ. – 2008. – № 2. – С. 46–53.
5. *Королев В.Ю.*, *Полиновский В.В.* Синтез портабельных информационных сервисов для флеш-накопителей // Там же. – 2008. – № 6. – С. 28–33.
6. *Корольов В.Ю.*, *Поліновський В.В.* Концепція побудови персоналізованих флеш-накопичувачів даних з апаратним захистом інформації // Математичні машини і системи. – 2009. – № 4. – С. 96–105.
7. *Королев В.Ю.* Алгоритмизация дистанционного распознавания ВІК-кода // Электронное моделирование. – 2008. – № 2. – С. 19–28.
8. *Корольов В.Ю.* Захист інформації в корпоративних *USB*-флеш накопичувачах для хмарних обчислень // Математичні машини і системи. – 2012. – № 2. – С. 60–69.
9. *Андерсон Дж.* Дискретная математика и комбинаторика. – К.: Вильямс, 2004. – 958 с.

Поступила 26.11.2012
Тел. для справок: +38 044 526-5585, 295-0851, 526-5585, 544-4667, +38 050 609-0234, +38 063 258-3226, +38 067 538-6890 (Киев)
E-mail: *dshv*937*@meta.ua*, *V.Polinovskyi@tau-systems.org.ua*