

УДК 621.391.7

© 2011 г. А. Л. Чмора

### МАСКИРОВКА КЛЮЧА С ПОМОЩЬЮ БИОМЕТРИИ

Построена абстрактная модель на основе фундаментального свойства однородности, учитывающая параметрические зависимости и отражающая специфический набор требований. Рассматривается метод маскировки криптографического ключа с помощью биометрии, удовлетворяющий построенной модели, а также гарантирующий адекватный уровень практической криптостойкости.

#### § 1. Введение

Использование биометрии в качестве секретного ключа в криптографических приложениях представляется логичным. Суть практической привлекательности биометрии как криптографического инструмента заключается в ее естественной *неотторжимости*. Действительно, любой криптографический ключ должен сохраняться в секрете. В практических приложениях ключ записывают на автономный носитель. Когда возникает необходимость, носитель подключается к криптографическому устройству с помощью предусмотренного для этих целей интерфейса. Ключ вводится в устройство путем считывания с носителя. Очевидно, что носитель не является неотъемлемой частью владельца ключа и легко может быть отторгнут. Например, потерян, украден или уничтожен.

Обозначенное свойство отторжимости критично для ряда приложений. Известно, например, что цифровая подпись гарантирует неотрекаемость. Целевое назначение этой услуги безопасности состоит в разрешении конфликтов, которые возникают в случае отказа от заверенного цифровой подписью документа, что означает, по сути, отказ от ранее взятых на себя обязательств. Всегда можно доказать, кто является автором цифровой подписи. Для этого достаточно предъявить открытый ключ, подлинность и уникальность которого подтверждена сертификатом, а также сам документ и его цифровую подпись. Ответчик раскрывает парный секретный ключ по постановлению суда. Однако в этой ситуации ответчик может воспользоваться свойством отторжимости и утверждать, что носителем, на котором хранится секретный ключ для вычисления подписи, воспользовались без его ведома. Как следствие, разбирательство усложняется. Теперь вместо установления авторства необходимо доказать или опровергнуть факт утечки секретной информации. При использовании биометрии обоснованность подобной аргументации вызовет справедливое сомнение.

Существуют и недостатки. Человек располагает ограниченным числом биометрических объектов определенного типа – десять пальцев на руках, два глаза, две ладони и т.д. Более того, биометрические объекты в силу известных ограничений не обладают гибкостью криптографических ключей, которые можно создавать многократно или даже увеличивать или уменьшать их энтропию, если изменились требования криптостойкости. Еще один недостаток связан с тем, что биометрия подвержена изменчивости и результаты измерения одного и того же объекта варьируются в некотором диапазоне. Как правило, подобная изменчивость носит кратковремен-

ный характер и зависит от факторов внешней среды. Однако с течением времени она может стать необратимой.

Биективность криптографического отображения возможна только тогда, когда ключ не изменяется в пределах одного цикла, состоящего из последовательного применения прямого и обратного криптографических преобразований. По этой причине биометрические данные невозможно использовать в качестве криптографического ключа. Решение проблемы тем не менее существует. Известны различные способы связывания биометрических данных и криптографического ключа [1–6]. Обзор приводится в § 2.

## § 2. Биометрия и криптографические ключи

Разъясним некоторые базовые понятия из области биометрии. Чаще всего биометрия применяется в задачах разграничения доступа. Биометрический эталон  $T$  – обобщенная характеристика, полученная в результате последовательности измерений и обработки множества проекций одного и того же биометрического объекта. Биометрический эталон формируется на этапе регистрации и сохраняется в долговременной памяти. Биометрический образ  $S$  – характеристика, полученная в результате текущего, как правило, однократного измерения биометрического объекта. Образ формируется в ходе запроса на предоставление доступа и предъявляется для распознавания относительно эталона. Необходимо отметить, что в общем случае эталон и образ могут быть получены от различных биометрических объектов.

Результаты распознавания оцениваются с помощью решающего правила. Если образ и эталон *однородны*, т.е. получены от одного и того же биометрического объекта, то правило выдает положительное заключение. Подчеркнем, что для фиксированного биометрического объекта может быть получено множество однородных образов и эталонов.

Отрицательное заключение указывает на то, что связь образа и эталона с конкретным биометрическим объектом не установлена. Тогда с большой вероятностью можно предположить, что образ и эталон *неоднородны*, т.е. получены от различных биометрических объектов.

Методы биометрической аутентификации позволяют принимать решение с некоторой вероятностью в пределах доверительного интервала. Надежность решения определяется ошибками первого и второго рода. В биометрии эти ошибки принято обозначать *False Rejection Rate* (FRR) и *False Acceptance Rate* (FAR) [7]. Таким образом, если решающее правило выдает одно из двух возможных заключений, например, *да* (свой) или *нет* (чужой), то FRR можно интерпретировать как ложноотрицательное срабатывание, или вероятность распознать своего как чужого, а FAR – как ложноположительное срабатывание, или вероятность распознать чужого как своего. Для существующих приложений важно, чтобы FAR была по возможности минимальной.

Ниже приводится краткий обзор способов связывания биометрических данных и криптографического ключа [1–6].

В [5] описан способ на основе ручного ввода с помощью клавиатуры. Ключ формируется как комбинация двоичного представления характеристической последовательности, описывающей динамику ввода, и пароля. В работе [2] аналогичная методология использована для представления ключа на основе голосовых характеристик. Переход к биометрии другого типа позволил увеличить энтропию ключа до 46 двоичных разрядов и снизить FAR до 20% [2].

Рукописный ввод исследовался в работе [4]. Были выделены 43 динамических признака, такие, например, как скорость, давление, направление и т.д. Затем признаки представлялись в виде двоичных последовательностей. Результирующий ключ

формировался как конкатенация этих последовательностей. В результате FAR и FRR составили 1,2% и 28% соответственно, а энтропия ключа не превысила 40 двоичных разрядов [4].

В [6, 8, 9] приводится описание способа выработки ключа с использованием отпечатков пальцев. В дальнейшем разработанная технология трансформировалась в коммерческий продукт под названием *Bioscrypt* ([www.bioscrypt.com](http://www.bioscrypt.com)). Преобразование Фурье применялось для выделения фазовой информации (доминирующего признака) из сканированного изображения отпечатка пальца. Изменчивость признака компенсировалась за счет мажоритарного декодирования. Основное отличие предложенного способа заключалось в маскировке ключа биометрическим эталоном. Было показано, что выделение ключа возможно с помощью однородного образа. Еще один способ с использованием отпечатков пальцев описан в [1]. Упомянутый способ в существенной степени опирается на идею работы [10]. Результирующий ключ формировался на основе особых точек с помощью полиномиальной интерполяции. Кроме того, для дополнительной маскировки применялись вспомогательные точки. Выделение ключа возможно в результате предъявления однородного эталона с близким набором особых точек. Расхождения, связанные с изменчивостью биометрического объекта, компенсировались с помощью кода Рида – Соломона. Авторам удалось обеспечить энтропию ключа на уровне 69 двоичных разрядов. При этом FRR составила 30%.

Для формирования криптографического ключа также использовалась биометрия человеческого лица [3]. Получен 80-разрядный ключ и 0,93% FAR.

### § 3. Модель

Обобщим известные подходы, краткий обзор которых приведен в § 2. С этой целью представим задачу в терминах абстрактной модели, учитывающей параметрические зависимости и отражающей специфический набор требований.

В дальнейших рассуждениях будем придерживаться трактовки однородности из § 2. Пусть заданы множества образцов  $\mathfrak{S}$  и эталонов  $\mathfrak{T}$ . Поскольку образ  $S$  всегда распознается относительно эталона  $T$ , и в каждой такой операции задействована отдельная пара, то введение прямого произведения вида

$$\mathfrak{S} \times \mathfrak{T} = \{(S, T) \mid S \in \mathfrak{S} \text{ и } T \in \mathfrak{T}\}$$

представляется логически обоснованным. Формально однородность определяется некоторой функцией  $h(\cdot, \cdot)$ . Образец  $S$  и эталон  $T$  однородны, если  $h(T, S) = \delta$  и  $\sigma > \delta \geq 0$ , где  $\sigma$  – наперед заданное пороговое значение.

Для указания на однородность образа и эталона воспользуемся знаком “ $\rightleftharpoons$ ”, а знаком “ $\neq$ ” – для неоднородности. Зафиксируем биометрический объект  $\mathcal{B}$  и рассмотрим  $r$  реализаций эталона  $T_j \in \mathbb{T}_{\mathcal{B}}$  и  $m$  реализаций образа  $S_i \in \mathbb{S}_{\mathcal{B}}$ , где  $\mathbb{S}_{\mathcal{B}} \subseteq \mathfrak{S}$ ,  $\mathbb{T}_{\mathcal{B}} \subseteq \mathfrak{T}$  и  $1 \leq j \leq r$ ,  $1 \leq i \leq m$ . Тогда

$$((\forall S_i \in \mathbb{S}_{\mathcal{B}}) \wedge (\forall T_j \in \mathbb{T}_{\mathcal{B}})) S_i \rightleftharpoons T_j$$

и

$$((\exists S_i \notin \mathbb{S}_{\mathcal{B}}) \vee (\exists T_j \notin \mathbb{T}_{\mathcal{B}})) S_i \neq T_j.$$

Более того,  $S_a \rightleftharpoons S_b$  и  $T_c \rightleftharpoons T_d$  при  $a \neq b$ ,  $c \neq d$ . Определим множества

$$\mathbb{S}_{\mathcal{B}} \times \mathbb{T}_{\mathcal{B}} = \{(S_i, T_j) \mid S_i \in \mathbb{S}_{\mathcal{B}} \text{ и } T_j \in \mathbb{T}_{\mathcal{B}}\},$$

$$\mathbb{S}_{\mathcal{B}} \times \mathbb{S}_{\mathcal{B}} = \{(S_a, S_b) \mid S_a, S_b \in \mathbb{S}_{\mathcal{B}}\},$$

$$\mathbb{T}_{\mathcal{B}} \times \mathbb{T}_{\mathcal{B}} = \{(T_c, T_d) \mid T_c, T_d \in \mathbb{T}_{\mathcal{B}}\}.$$

Следовательно, для объекта  $\mathcal{B}$  множество однородных образов и эталонов определяется как

$$\mathfrak{U}_{\mathcal{B}} = (\mathbb{S}_{\mathcal{B}} \times \mathbb{T}_{\mathcal{B}}) \cup \mathbb{S}_{\mathcal{B}}^2 \cup \mathbb{T}_{\mathcal{B}}^2.$$

Отметим также коммутативные свойства, а именно, если  $S \rightleftharpoons T$  или  $S \not\rightleftharpoons T$ , то  $T \rightleftharpoons S$  или  $T \not\rightleftharpoons S$  соответственно.

Кроме этого, если  $S_X \rightleftharpoons T_Y$  и  $T_Y \rightleftharpoons T_Z$ , то  $S_X \rightleftharpoons T_Z$ ,  $T_Y \neq T_Z$ . Аналогично, если  $S_X \rightleftharpoons S_Y$  и  $S_Y \rightleftharpoons T_Z$ , то  $S_X \rightleftharpoons T_Z$ ,  $S_X \neq S_Y$ .

Пусть задан криптографический ключ  $K$  и произвольные  $S, T$ . Введем следующую пару преобразований:  $\mathcal{M} = f(T, K)$  и  $\mathcal{K} = g(\mathcal{M}, S)$ . Положим  $\gamma = \log_2 \mathcal{M}$  и  $\lambda = \log_2 K$ .

Рассмотрим ряд условий и предположений, составляющих основу модели.

1.  $f(\cdot, \cdot)$ ,  $g(\cdot, \cdot)$  и  $\mathcal{M}$  общедоступны;
2. Если  $S \rightleftharpoons T$ , то  $\mathcal{K} = K$ ;
3. Если  $S \not\rightleftharpoons T$ , то  $\mathcal{K} \neq K$ ;
4. При известных  $T$  и  $K$  значение  $\mathcal{M}$  вычисляется со сложностью  $O(\lambda^\alpha)$ ,  $\alpha > 1$ ;
5. Для заданного  $S$ ,  $S \rightleftharpoons T$ , ключ  $K$  вычисляется со сложностью  $O(\lambda^\beta)$ ,  $\beta \geq \alpha$ ;
6. Для заданного  $S$ ,  $S \not\rightleftharpoons T$ , ключ  $K$  вычисляется со сложностью  $O(\exp(\gamma))$ ;
7. При известном  $T$  ключ  $K$  вычисляется со сложностью  $O(1)$ ;
8. При неизвестном  $T$  ключ  $K$  вычисляется со сложностью  $O(\exp(\gamma))$ .

Согласно уловию 7 ключ  $K$  и эталон  $T$  должны сохраняться в секрете. Из 5 следует, что образ  $S$  также должен сохраняться в секрете.

Предположим, что секретность определяется наличием *зоны относительной неуязвимости*, которая ограничена периметром безопасности. Если операционная активность осуществляется в пределах такой зоны, то минимизируются риски, связанные с раскрытием секретной информации. Отсюда следует, что формирование  $T$  и  $S$ , генерацию ключа  $K$ , а также выделение  $K$  из  $\mathcal{M}$  при заданном  $S$  необходимо выполнять в пределах обозначенной зоны.

В дальнейшем будем исходить из следующих предположений.

- Доверенная сторона отвечает за регистрацию, генерацию ключа  $K$ , формирование эталона  $T$ , а также  $\mathcal{M}$ . Операционная активность доверенной стороны ограничена пределами зоны относительной неуязвимости.
- Значение  $\mathcal{M}$  заносится в специализированную базу данных для долговременного хранения. База данных размещается вне зоны относительной неуязвимости и соответственно подвержена атакам.
- В ходе формирования образа  $S$  может быть предъявлен не тот биометрический объект, который использовался при формировании эталона  $T$ .
- В ходе формирования образа  $S$  может быть предъявлен не биометрический объект, а артефакт.
- Операционная активность на этапе распознавания образа  $S$  относительно эталона  $T$  и принятия решения по результатам распознавания осуществляется в пределах зоны относительной неуязвимости.

**3.1. Анализ.** Выполним анализ модели в контексте методов теории помехоустойчивого кодирования.

Пусть криптографический ключ  $K$  трактуется как информационные символы линейного  $k$ -мерного кода  $\mathcal{C}$  с минимальным расстоянием  $d$  [11]. Код  $\mathcal{C}$  задан порождающей матрицей  $G$  размера  $k \times n$ . Тогда существует кодовое слово  $\mathbf{c} = KG$ ,  $\mathbf{c} \in \ker(H)$ , где  $H$  – проверочная матрица размера  $(n-k) \times n$  кода  $\mathcal{C}$ . Биометрический эталон  $T$ , созданный на этапе регистрации, рассматривается как вектор ошибки  $\mathbf{e}$  для кодового слова  $\mathbf{c}$ . Сумма  $\mathcal{M} = \mathbf{c} + \mathbf{e} = KG \oplus T$  сохраняется в долговременной базе данных.

Ключ  $K$  выделяют из  $\mathcal{M}$ , когда в этом возникает необходимость. Например, для выполнения зашифрования/расшифрования. Для этого необходимо получить образ  $S$  того биометрического объекта, который использовался для создания эталона  $T$ .

1. Если  $T \simeq S$ , то  $\text{wt}(T \oplus S) < (d - 1)/2$ . Как следствие, код  $\mathcal{C}$  способен исправить  $T \oplus S$  ошибок. Ключ  $K$  будет получен в результате декодирования с исправлением ошибок.
2. Если  $T \not\simeq S$ , то  $\text{wt}(T \oplus S) > (d - 1)/2$ , и ключ  $K$  не будет получен, так как  $\mathcal{C}$  не сможет исправить ошибки.

Таким образом, для  $T \simeq S$  получение ключа  $K$  не сопряжено с высокими вычислительными трудозатратами. Если  $T \not\simeq S$ , то вес вектора ошибки превышает  $(d - 1)/2$ , и декодирование с исправлением ошибок невозможно. В частности, доказано, что декодирование случайного кода по максимуму правдоподобия, эквивалентное в нашем случае декодированию в ближайшее кодовое слово, относится к классу  $NP$ -трудных проблем [12–15]. Кроме того, показано, что декодирование по максимуму правдоподобия даже для конкретных семейств случайных кодов, например, кодов Рида–Соломона, также относится к классу  $NP$ -трудных проблем [16].

С другой стороны, для кодов Рида–Соломона разработан алгоритм декодирования полиномиальной трудоемкости, который позволяет исправлять ошибки веса  $t > (d - 1)/2$ . В литературе этот алгоритм известен как алгоритм Гурусвами–Судана [17]. Однако конфликта с моделью не возникает. Поясним, почему это так.

Во-первых, полиномиальная сложность декодирования  $t$  ошибок быстро возрастает с увеличением разности  $\Delta = t - (d - 1)/2$ .

Во-вторых, существует верхняя граница числа ошибок  $t$ , для которой декодирование невозможно. В частности, для алгоритма Гурусвами–Судана такая граница –

$$t \leq n \left( 1 - \sqrt{1 - \frac{d}{n}} \right) < d.$$

В-третьих, как будет показано в § 5, для скорости кода  $k/n \sim 1/4$  величина  $\Delta$  весьма незначительна.

В-четвертых, безусловно, можно воспользоваться алгоритмом Гурусвами–Судана для исправления  $t > (d - 1)/2$  ошибок для  $T \simeq S$ . Однако несложно подобрать параметры таким образом, что декодирование с исправлением ошибок по алгоритму Гурусвами–Судана станет невозможным.

Следует отметить, что распределение суммы  $T \oplus S$ , как правило, отлично от равномерного. В частности, распределение веса Хэмминга зависит от типа биометрии и способа ее обработки. Если предположить, что образы/эталон биометрического объекта  $\mathcal{B}$  представлены последовательностями из  $m$  двоичных разрядов, то  $|\mathbb{S}_{\mathcal{B}} \times \mathbb{T}_{\mathcal{B}}| < 2^m$ . Если цель атаки – раскрытие секретного ключа  $K$  при заданном  $\mathcal{M}$ , то оптимальная стратегия сводится к перебору вариантов из множества  $\mathbb{S}_{\mathcal{B}}$  при условии, что атакующий способен порождать различные образы в автоматическом режиме с приемлемой трудоемкостью. Очевидно, что успех подобной атаки зависит от типа биометрии и ее свойств и не зависит от прогресса в области декодирования линейных кодов.

В завершение отметим, что приведенные выше рассуждения справедливы, если биометрия обладает специальными статистическими свойствами. Установлено, что к биометрии такого типа относится радужная оболочка глаза человека.

#### § 4. Статистические свойства радужной оболочки

Исследовались свойства радужной оболочки глаза для задач биометрической идентификации, когда заданный образ  $S$  распознается относительно множества эталонов  $T_i$  [18, 19]. Результаты продемонстрировали строгую статистическую незави-

симость в случае  $T_i \neq S$  и устойчивую корреляцию при  $T_i \Leftrightarrow S$ . Кратко остановимся на этих результатах.

Для представления образа в двоичном виде применялся следующий метод. Локальные области изображения радужной оболочки глаза представлялись с помощью двумерной вейвлет-спектрограммы преобразования Габора [20]. Координаты радиус-вектора на комплексной плоскости задавались вещественной и мнимой частями комплекснозначных коэффициентов преобразования. Затем вектор квантовался одним из четырех квадрантов (1/4 окружности) комплексной плоскости, каждому из которых были приписаны два двоичных разряда. Векторы с координатами, которые задавались положительными мнимой и вещественной частями, кодировались как 11, положительной вещественной и отрицательной мнимой – 10, отрицательными вещественной и мнимой – 00, положительной мнимой и отрицательной вещественной – 01. В результате формировалась последовательность из  $2^{11}$  двоичных разрядов, которая сохранялась в памяти.

Первый статистический эксперимент заключался в попарном сравнении неоднородных образов из тестового набора данных. В качестве *меры несходства*  $n$ -разрядных векторов  $x$  и  $y$  использовалось нормированное расстояние Хэмминга  $\mathcal{H} = \text{wt}(x \oplus y)/n$ . В качестве нулевой была выбрана гипотеза о статистической независимости неоднородных образов. Известно, что для статистически независимых двоичных переменных  $\text{Prob}\{0\} = \text{Prob}\{1\} = 1/2$ . Тогда для пары неоднородных образов  $\mathcal{H} = 0,500$ .

Тестовый набор состоял из 4258 неоднородных образов. Всего было выполнено немногим более 9 миллионов попарных сравнений. Зависимость меры несходства от числа попарных сравнений была представлена в виде гистограммы со средним  $\mathcal{H}^{\text{cp}} = 0,499$ ,  $\mathcal{H}^{\text{min}} = 0,334$ ,  $\mathcal{H}^{\text{max}} = 0,664$  и стандартным отклонением  $\sigma = 0,0317$ . Полученная гистограмма соответствует биномиальной функции распределения с  $p = 0,5$  и  $N = p(1 - p)/\sigma^2 = 249$  степенями свободы

$$f(\xi) = \frac{N!}{m!(N - m)!} p^m (1 - p)^{N - m}, \quad (1)$$

где  $\xi = m/N$  – доля успехов в  $N$  испытаниях Бернулли. В контексте описанного статистического эксперимента величина  $\xi = (1 - \mathcal{H})n$  есть *мера сходства* пары образов, представленных  $n$ -разрядными двоичными векторами.

Экспериментально установлено, что при сравнении неоднородных образов различаются не менее трети двоичных разрядов. Тогда  $\text{Prob}\{\exists \mathcal{H} \mid 0 \leq \mathcal{H} < 0,333\} < 2^{-24}$  и  $\text{Prob}\{\exists \mathcal{H} \mid 0 \leq \mathcal{H} < 0,300\} < 2^{-30}$ . Таким образом, была подтверждена гипотеза о статистической независимости неоднородных образов и доказано, что каждый двоичный разряд образа есть суть результат испытания Бернулли с параметром  $p = 0,5$  и  $N = 249$ .

Цель второго эксперимента – исследование статистических свойств однородных образов. Для этого были сформированы два различных тестовых набора из 7070 пар. Образы, полученные в результате сканирования одного и того же объекта с помощью различных моделей сканирующей камеры, расстояния до объекта, освещенности и так далее, сохранялись в тестовом наборе  $\mathcal{B}_1$ . В тестовом наборе  $\mathcal{B}_2$  сохранялись однородные образы, полученные с помощью одного и того же сканирующего устройства с фиксированными фокусным расстоянием, освещенностью и расстоянием до объекта. Построены распределения меры несходства со средним  $\mathcal{H}_1^{\text{cp}}$ , стандартным отклонением  $\sigma_1$  для  $\mathcal{B}_1$  и  $\mathcal{H}_2^{\text{cp}}$  и  $\sigma_2$  для  $\mathcal{B}_2$  (см. таблицу). В ходе эксперимента установлено, что  $\mathcal{H}_2 = 0$  для половины всех попарных сравнений из  $\mathcal{B}_2$ .

В третьем эксперименте однородные образы из  $\mathcal{B}_1$  и  $\mathcal{B}_2$  сравнивались с неоднородными образами из тестового набора первого эксперимента. Параметры распределения меры несходства для третьего эксперимента  $\tilde{\mathcal{H}}^{\text{cp}}$  и  $\tilde{\sigma}$  также представлены в

Таблица

Параметры распределений для тестовых наборов  $\mathcal{B}_1$  и  $\mathcal{B}_2$ 

$\mathcal{B}_1$	$\mathcal{B}_2$
$\mathcal{H}_1^{\text{cp}} = 0,110$	$\mathcal{H}_2^{\text{cp}} = 0,019$
$\sigma_1 = 0,065$	$\sigma_2 = 0,039$
$\tilde{\mathcal{H}}_1^{\text{cp}} = 0,456$	$\tilde{\mathcal{H}}_2^{\text{cp}} = 0,458$
$\tilde{\sigma}_1 = 0,020$	$\tilde{\sigma}_2 = 0,0197$

таблице. Показано, что  $\mathcal{H}_1^{\text{max}} = 0,327$  при попарном сравнении однородных образов из  $\mathcal{B}_1$ , тогда как при сравнении образов из  $\mathcal{B}_1$  с образами из тестового набора первого эксперимента  $\tilde{\mathcal{H}}_1^{\text{min}} = 0,329$ . Хвосты двух распределений не пересекаются, что гарантирует однозначность заключений решающего правила. Анализ полученных распределений показал, что при сравнении однородных образов параметры распределения находятся в существенной зависимости от условий сканирования. Однако для неоднородных образов параметры распределения практически не зависят от условий сканирования. Последнее означает, что использование данной биометрии гарантирует низкую FAR.

Дополнительные исследования с привлечением обширных экспериментальных данных [21] подтвердили установленные ранее свойства радужной оболочки глаза.

### § 5. Пример кодовой конструкции

Свойства биометрии из § 4 хорошо согласуются с моделью из § 3. Приведем пример кодовой конструкции. Для этого выберем двоичный код БЧХ с  $n = 2048$  размерности  $k \geq 398$ , исправляющий двоичные ошибки веса  $t \leq 150$ . В соответствии с распределением, полученным в первом эксперименте, вероятность успешного распознавания своего превысит 80%. Для  $T \neq S$  вероятность распознавания чужого как своего меньше  $10^{-45} \approx 2^{-135}$  при условии, что  $\text{wt}(T \oplus S) \leq 150$ . Тогда FAR  $\sim 2^{-135}$  и FRR  $\sim 0,8$ . В случае неоднородности  $\text{wt}(T \oplus S) > 301$  с вероятностью  $> 1 - 10^{-30}$ , что превышает конструктивное расстояние кода БЧХ. Трудоемкость лучшего из известных алгоритмов декодирования оценивается как  $2^{140}$  операций над двоичными символами [22]. Следует отметить, что в большинстве случаев в результате декодирования будет получено неправильное кодовое слово.

### § 6. Постановка задачи

На основании обзора, представленного в § 2, можно заключить, что известные решения либо не удовлетворяют модели из § 3, либо не позволяют получить достаточного количества энтропийных разрядов. Если исходить из пессимистичной оценки, то при использовании симметричного криптографического преобразования гарантированная криптостойкость обеспечивается при энтропии ключа не менее 128 двоичных разрядов. С другой стороны, приведенные в [23–26] прогнозы отражают практический подход к оценке криптостойкости.

Вышеизложенные соображения позволяют сформулировать следующую постановку задачи.

*Необходимо разработать метод маскировки криптографического ключа с помощью биометрии, удовлетворяющий модели из § 3 и гарантирующий адекватный уровень практической криптостойкости согласно [23–26].*

Отметим, что биометрия конкретного типа занимает определенное положение как в прикладном смысле, так и в смысле разнообразия технологических решений. Тогда применение биометрии иного типа, отличного от перечисленных в § 2, следует, безусловно, расценивать как качественное достижение.

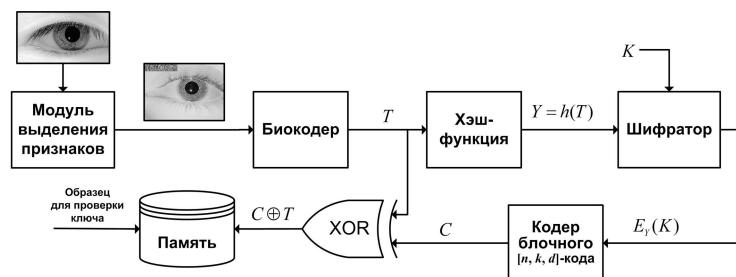


Рис. 1. Представление ключа

## § 7. Метод биометрической вуали

Дадим описание метода *биометрической вуали* [27, 28], удовлетворяющего модели из § 3. Метод в существенной степени использует свойства биометрии из § 4. Отметим, что аналогичный подход предложен в [29].

**7.1. Представление криптографического ключа.** Для представления криптографического ключа выполняются следующие действия (см. рис. 1).

1. Получают набор данных в результате последовательности измерений и обработки множества проекций одного и того же биометрического объекта.
2. На основании полученных данных формируют эталон  $T$ .
3. С помощью случайного процесса или генератора псевдослучайных чисел генерируют криптографический ключ  $K$ .
4. Формируют тестовый образец для проверки ключа. Например,  $\hat{K} = h(K)$ , где  $h(\cdot)$  – криптографическая хэш-функция. Тестовый образец сохраняют в долговременной памяти.
5. Вычисляют значение криптографической хэш-функции от эталона  $Y = h(T)$ .
6. Ключ  $K$  зашифровывают с помощью  $Y$ . В результате получают шифротекст  $X = E_Y(K)$ , где  $E_Y(\cdot)$  – функция зашифрования.
7. В кодере блочного кода выполняют кодирование шифротекста  $X$  блочным  $(n, k, d)$ -кодом с целью получения кодового слова  $C$ .
8. Вычисляют поразрядную сумму  $C \oplus T$ . Предполагается, что число разрядов двоичного представления  $C$  совпадает с числом разрядов  $T$ .
9. Сохраняют результат суммирования в долговременной памяти.

**7.2. Выделение криптографического ключа.** Для выделения криптографического ключа выполняется следующая последовательность шагов (см. рис. 2).

1. Получают данные по меньшей мере от одного биометрического объекта.
2. Формируют в блоке выделения признаков и биокодере образ  $S$ .
3. Извлекают из долговременной памяти сумму  $C \oplus T$ .
4. Вычисляют поразрядную сумму  $C_{\text{ош}} = C \oplus T \oplus S$ . Отметим, что после суммирования кодовое слово  $C_{\text{ош}}$  все еще может содержать ошибки.
5. Выполняют конструктивное декодирование  $C_{\text{ош}}$ . Исход декодирования зависит от веса вектора ошибки. Возможны следующие три события:
  - I. *Вес вектора ошибки не превышает  $t$ .* Это означает, что  $T \approx S$ . Ошибки будут исправлены в декодере блочного кода, информационные символы  $X$  восстановлены корректно;
  - II. *Вес вектора ошибки незначительно превышает  $t$ .* Однако ошибка данного веса не может быть исправлена. В этом случае на специальном выходе декодера блочного кода формируется признак отказа от декодирования, который указывает на  $T \neq S$  или сигнализирует о погрешностях сканирования биометрического объекта;

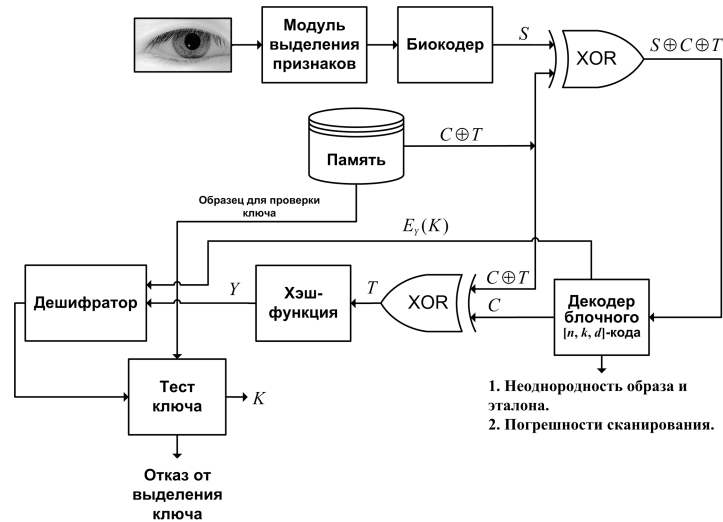


Рис. 2. Выделение ключа

III. Вес вектора ошибки значительно превышает  $t$ . Это означает, что  $T \neq S$ . В этом случае декодер блочного кода принимает решение об исправлении ошибок меньшего веса в другом, отличном от  $C_{\text{ош}}$ , кодовом слове и вместо  $X$  восстанавливает случайную последовательность информационных символов. Событие опосредованно обнаруживается на шаге 10.

6. Предположим, что вес вектора ошибки не превышает  $t$ . В результате декодирования получают исправленное кодовое слово  $\hat{C}_{\text{ош}}$ .
7. Извлекают  $C \oplus T$  из долговременной памяти и вычисляют поразрядную сумму  $T = \hat{C}_{\text{ош}} \oplus (C \oplus T)$ .
8. Вычисляют значение хэш-функции  $Y = h(T)$ .
9. Выделяют криптографический ключ  $K = D_Y(X)$ , где  $D_Y(\cdot)$  – функция расшифрования.
10. Подтверждают корректность выделенного ключа. С этой целью извлекают тестовый образец для проверки ключа из долговременной памяти и проверяют справедливость равенства  $\hat{K} \stackrel{?}{=} h(K)$ . Если равенство подтверждено, то на специальном выходе формируется признак отказа от выделения ключа.

**7.3. Анализ криптостойкости.** Выполним анализ криптостойкости метода биометрической вуали. Выберем  $C \oplus T$  в качестве объекта криптоанализа. Существует несколько причин, по которым выгоднее воспользоваться силовой атакой с целью получения эталона  $T$ .

1. Эталон  $T$  – уникальная биометрическая характеристика, которую в случае компрометации не всегда просто заменить другой аналогичной по свойствам.
2. Декодирование  $C \oplus T = C + e$  практически неосуществимо, так как  $\text{wt}(e) \gg \gg (d - 1)/2$ . Обоснование приведено в п. 3.1.
3. Если ключ  $K$  – случайная равномерно распределенная последовательность из  $k$  двоичных разрядов, то на выходе кодера блочного  $(n, k, d)$ -кода с равной вероятностью может появиться любое из  $2^k$  кодовых слов. Следовательно, энтропия суммы  $C \oplus T$  не более  $k$ . Обоснованной представляется пессимистическая оценка энтропии  $\ell$  эталона  $T$ , когда  $\ell < k$ . Тогда в среднем понадобится выполнить не более  $2^{\ell-1}$  проверок.

4. Возможно использование эталона  $T$  в различных приложениях. Тогда общедоступны несколько сумм  $C_1 \oplus T, C_2 \oplus T, \dots, C_m \oplus T$ , таких что  $C_i \neq C_j$  для всех  $i \neq j$ . Если  $T$  известно, то несложно получить все  $K_i, i = \overline{1, m}$ .

**Силовая атака.** Под силовой атакой будем понимать метод проб и ошибок с исчерпывающим перебором вариантов. Для успеха необходимо сформулировать критерий выбраковки претендентов. С этой целью разумно воспользоваться ключом  $K$ . Обоснуем этот выбор. При известном  $X = E_Y(K)$  несложно вычислить  $C$  и  $T$ . Отметим, что  $X$  присутствует в памяти устройства в течение короткого промежутка времени, тогда как ключ  $K$  используется для зашифрования/расшифрования значительных объемов информации и в большей степени подвержен компрометации. Также возможно использование тестового образца для проверки ключа  $\tilde{K} = h(K)$ . Действительно, если автономный носитель доступен на чтение, то злоумышленник может скопировать  $C \oplus T$  и  $\tilde{K}$  без ведома владельца (см. п. 7.1).

Для того чтобы определить  $T$  при известном  $K$ , необходимо вычислить  $X$ , но для этого необходимо знать  $T$ . Следовательно, при известном  $K$  и неизвестном  $T$  невозможно вычислить  $X$ .

Предположим, декодер исправляет ошибки веса  $t < (d-1)/2$ . Обозначим образ претендент через  $\tilde{S}$ , отличное от  $C$  кодовое слово обозначим через  $\check{C}$ ,  $\tilde{K} = D_{\tilde{Y}}(\tilde{X})$ , где  $\tilde{Y} = h(\tilde{T})$ . Испытание каждого претендента сопровождается проверкой следующих гипотез.

- I.  $C \oplus T \oplus \tilde{S} = \check{C}$ .
- II.  $C \oplus T \oplus \tilde{S} = \check{C}$ .
- III.  $C \oplus T \oplus \tilde{S} = \check{C} + \mathbf{e}, t < (d-1)/2$ .
- IV.  $C \oplus T \oplus \tilde{S} = C + \mathbf{e}, t < (d-1)/2$ .

Подтверждение гипотез II и IV указывает на факт получения эталона  $T$ . При этом гипотеза II соответствует случаю  $\tilde{S} = T$  и декодированию без исправления ошибок, а гипотеза IV – декодированию с исправлением ошибок, когда  $\text{wt}(T \oplus \tilde{S}) < (d-1)/2$ . Поскольку вектор ошибки  $\mathbf{e} = T \oplus \tilde{S}$  известен в результате декодирования, то легко вычислить  $T = \tilde{S} \oplus \mathbf{e}$ . Однако по результатам декодирования невозможно отделить гипотезу II от I, а также гипотезу IV от III. Тогда равенство  $K = \tilde{K}$  свидетельствует о подтверждении гипотезы II или IV, а  $K \neq \tilde{K}$  – о подтверждении гипотезы I или III.

Согласно распределению (1) (см. § 4) имеем  $\ell = 249$ . Уточним, однако, что эта оценка энтропии отражает результаты конкретного эксперимента и может меняться по мере накопления статистических данных.

**Трудоёмкость силовой атаки.** Отдельное испытание в ходе силовой атаки состоит из следующих шагов.

1. Синтез претендента  $\tilde{S}$ .
2. Декодирование  $C \oplus T \oplus \tilde{S}$ . Получение  $\check{C}, \tilde{X}, \mathbf{e}$ .
3. Вычисление  $\tilde{T} = \tilde{S} \oplus \mathbf{e}$ .
4. Вычисление  $\tilde{Y} = h(\tilde{T})$ .
5. Расшифрование  $\tilde{K} = D_{\tilde{Y}}(\tilde{X})$ .
6. Сравнение  $K \stackrel{?}{=} \tilde{K}$  или  $\tilde{K} \stackrel{?}{=} h(\tilde{K})$ .

Образ состоит из  $2^{11}$  двоичных разрядов. Энтропия образа, так же, как и эталона, не превышает 249 двоичных разрядов. Предположим, что известны все 249 позиций, на которых располагаются случайные и независимые символы. Предположим также, что этот набор позиций зафиксирован для всевозможных образов. Значения символов на остальных позициях образа могут быть вычислены с приемлемой трудоёмкостью. Сделаем упрощающее предположение о расположении на

этих позициях символов с нулевыми значениями. Следовательно, если заданы два различных образа  $S_1$  и  $S_2$ , то  $\text{wt}(S_1 \oplus S_2) \leq 249$ .

Пусть имеется шаблон из  $2^{11}$  разрядов. Тогда простейший способ синтеза образа заключается в генерации двоичной последовательности, в которой не менее 249 символов энтропии, с последующим размещением значений символов из этой последовательности на известных позициях шаблона. Понятно, что при таком подходе силовая атака практически неосуществима, так как в среднем для поиска решения необходимо испытать  $2^{248}$  претендентов.

Можно поступить по-другому. Предположим, что код исправляет все двоичные ошибки веса  $t$  и меньше. Пусть задано кодовое слово с ошибками  $C_{\text{ош}} = C \oplus T$ . Очевидно, что значение, которое принимает символ на каждой из 249 позиций слова  $C_{\text{ош}}$ , есть результат суммирования случайного и кодового символов. Если код исправляет не более  $t$  ошибок, то можно изменить значения символов на произвольных  $t$  из известных 249 позиций и затем провести испытание (шаги 2, 3, 4, 5 и 6). Пусть задан список из 249 позиций. Чтобы изменить значения символов, достаточно сформировать шаблон  $\tilde{S}$  веса  $t$ , такой что его разрядность равна  $2^{11}$  и на позициях из списка расположены  $t$  единиц, а нули расположены на всех остальных позициях. Затем выполнить суммирование  $C_{\text{ош}} \oplus \tilde{S}$ . Тогда совокупное число испытаний не превысит  $\sum_{i=0}^t \binom{249}{i}$  попыток. Следует, однако, отметить, что при  $i = 10$  число испытаний не более  $2^{56}$ , но при  $i > 100$  число испытаний сравнимо с  $2^{248}$  и атака методом перебора ошибок веса  $t$  не имеет никаких преимуществ.

Возможно ли сократить объем перебора? Как было отмечено в § 4,  $\mathcal{H} \geq 0,333$  в случае  $T \neq \tilde{S}$ . Следовательно, можно ввести ограничение на  $t$  сверху, положив  $t = 83$ . Но уже при  $t = 16$  число испытаний приближается к  $2^{80}$ . Применительно к симметричной шифросистеме в [23, 30] показано, что при использовании 80-разрядного ключа силовая атака неосуществима на практике. Прогноз [23, 25, 30], выраженный в достаточной для обеспечения адекватной криптостойкости разрядности ключа, не связан с алгоритмической спецификой, а отражает тенденции роста производительности вычислительных платформ. Согласно [23–26] криптостойкость гарантируется при разрядности ключа от 75 до 80. Это означает, что в диапазоне  $10 < t \leq 83$  исчерпывающий перебор невозможен. Следовательно, с помощью перебора ошибок веса  $t$  можно проверить не более 9% от общего числа претендентов.

Оценим трудоемкость перебора как совокупное число двоичных операций при  $t = 10$ . В [24] указано, что 56-разрядный ключ обеспечивал высокий уровень криптостойкости в 1994 г., но такой ключ не может считаться надежным на современном этапе развития технологий. Трудоемкость отдельного испытания определяется вычислительной сложностью шагов 2, 4 и 5. Известно, что вычислительная сложность алгоритма синдромного декодирования алгебраического кода полиномиальна по  $n$ , и как правило, не превышает  $O(n^3)$ . Для примера из § 5 сложность декодирования – порядка  $2^{33}$  двоичных операций. Сложность расшифрования по алгоритму AES – порядка  $2^{10}$  двоичных операций на 128-разрядный блок [31]. Для вычисления значения хэш-функции по алгоритму SHA-256 потребуется не более  $2^{16}$  двоичных операций на 512-разрядный блок. Предположим, трудоемкость испытания не превышает  $2^{33}$  двоичных операций. Тогда трудоемкость перебора ошибок веса  $t = 10$  составит порядка  $2^{89}$  двоичных операций. Если производительность испытательного устройства 100 Гбит/с, то для поиска решения методом исчерпывающего перебора при  $t = 10$  понадобится не менее  $10^8$  лет. Очевидно, что уровень криптостойкости определяется типом приложения. Например, для сценария практического применения, описанного в § 8, такой уровень криптостойкости представляется обоснованным.

Если по каким-либо причинам  $\text{wt}(T \oplus S) \leq t_{\text{кр}}$ , где  $t_{\text{кр}}$  – число ошибок, при котором криптостойкость снижается до критического уровня, но при этом  $d$  достаточно

велико, например, такое, что  $t = 83$ , то можно повысить криптостойкость добавлением вспомогательного вектора ошибки  $M$ . Вектор  $M$  выбирается таким образом, чтобы вес Хэмминга суммы  $T \oplus S \oplus M$  приближался к корректирующей способности кода.

## § 8. Сценарий практического применения

Рассмотрим возможный сценарий практического применения метода биометрической вуали.

Предположим, необходимо организовать распространение цифрового контента, например аудио/видео продукции, с целью продажи удаленным потребителям. Для доставки контента разумно воспользоваться современными сетевыми технологиями. Для этого заявитель персонально является в офис компании, официально уполномоченной правообладателем контента, например, со статусом авторизованного дилера, и проходит регистрацию. Создается учетная запись, в которую заносятся его реквизиты. Затем с помощью преобразования  $f(T, K)$  вычисляется сумма  $C \oplus T$ , которая записывается на автономный носитель, например токен-устройство, а ключ  $K$  заносится в соответствующее поле учетной записи. Эталон  $T$  удаляется из памяти сразу же после вычисления  $C \oplus T$ . По факту регистрации автономный носитель передается заявителю. Удаленное потребление, например, посредством обращения к специализированному сетевому ресурсу с последующей загрузкой контента в устройство воспроизведения, осуществляется в пределах размещенных на персональном счете средств. Счет ассоциирован с учетной записью. Загрузка контента сопровождается списанием определенной суммы.

Для доступа к ресурсу необходимо пройти авторизацию, в результате которой идентифицируется учетная запись. Особенность заключается в том, что перед загрузкой контент зашифровывается с помощью ключа  $K$ , который предварительно извлекается из учетной записи. Для расшифрования с помощью преобразования  $g(C \oplus T, S)$  в устройство необходимо также ввести образ  $S$  и подключить автономный носитель с записанной ранее суммой  $C \oplus T$ . Предполагается, что устройство воспроизведения сконструировано таким образом, что скопировать полученный в результате расшифрования цифровой контент не представляется возможным. Отметим, что всегда возможно выполнить копирование данных на выходе устройства воспроизведения, подобно тому как можно сделать копию, воспользовавшись камерой для съемки фильма во время его показа. Однако качество полученной таким образом копии, как правило, значительно хуже оригинала. Встроенный биометрический сканер – еще одна конструктивная особенность устройства воспроизведения. Ввод данных в устройство возможен только с помощью специализированных интерфейсов.

**8.1. Способы распространения контента.** Для выяснения преимуществ метода биометрической вуали рассмотрим два способа распространения контента, которые в различных вариациях используются на практике. Регистрация, создание учетной записи и авторизация осуществляются в соответствии с приведенным выше описанием.

Способ 1. Предположим, что контент зашифровывается/расшифровывается с помощью ключа  $K$  без использования биометрии. При этом возрастает риск незаконного тиражирования. Действительно, существует возможность распространения зашифрованного контента вместе с ключом  $K$ . Несмотря на то, что подобные действия являются противозаконными и способны причинить значительный ущерб правообладателю, статистика нарушений авторских прав в сфере цифрового контента свидетельствует о массовости таких преступлений. Одна из причин – отторжимость ключевого носителя. Потребитель, например, может утверждать, что автономный носитель был либо украден, либо, если не существует технологических ограничений, копирование ключа было выполнено без его ведома. Затем скопированный ключ был

записан на новый носитель, которым и воспользовался злоумышленник. Не часто удается опровергнуть подобное утверждение. Еще одна причина, которую также следует отметить, это беззатратность процесса копирования информации.

Способ 2. Пусть в каждое устройство в процессе производства записывается уникальный секретный ключ асимметричной шифросистемы. Предположим, что этот ключ невозможно использовать вне устройства. Иными словами, криптографическое преобразование выполняется внутри устройства по факту ввода данных. Назовем такой ключ *неизвлекаемым*. Напомним, что асимметричное криптографическое преобразование предполагает наличие парного открытого ключа. Соответствующий открытый ключ генерируется одновременно с секретным, но в отличие от последнего общедоступен. Открытый ключ распространяется в виде сертификата, который выпускается доверенной стороной – удостоверяющим центром. Ключ  $K$  зашифровывается на открытом ключе устройства и передается потребителю. Для выделения ключа  $K$  необходимо выполнить расшифрование на парном секретном ключе. Отметим, что такое расшифрование возможно только в том устройстве, которое было заявлено в ходе регистрации, и невозможно во всех остальных. В итоге в памяти устройства сохраняется ключ  $K$ , который также неизвлекаем. Теперь контент, зашифрованный с помощью ключа  $K$ , может быть расшифрован только в данном устройстве. Поскольку ключ  $K$  неизвлекаем, то тиражирование невозможно.

**8.2. Сравнительный анализ.** Разберем метод биометрической вуали в контексте рассмотренных выше способов распространения контента.

Предположим, потребитель вознамерился растиражировать контент. Тогда помимо суммы  $C \oplus T$  он также должен обнародовать образ  $S$ . Однако образ  $S$  может быть получен только в результате сканирования объекта. Следовательно, понадобится каким-то образом воспроизвести реплику биометрического объекта (например, создать муляж). Даже если это технологически возможно, стоимость создания муляжа может быть достаточно высокой. Тогда логично предположить, что масштаб тиражирования будет зависеть от объема инвестиций. Важно то, что копирование информации перестает быть беззатратным, что безусловно является сдерживающим фактором. Кроме того, конечное число доступных биометрических объектов приводит к тому, что один и тот же объект используется в различных приложениях. Сложно представить, какой должна быть мотивация, чтобы осознанно обнародовать реплику объекта, который одновременно используется для расшифрования цифрового контента и доступа к банковской ячейке.

Второй из описанных способов позволяет решить проблему незаконного тиражирования. Однако существующие ограничения и относительно высокая стоимость решения препятствуют практическому применению. Поясним, о чем идет речь.

Доставка открытых ключей в удостоверяющие центры с целью выпуска сертификата существенно усложняет производственный цикл и связана с дополнительными накладными расходами. Установленные правила и процедуры доставки ключей вытекают из фундаментальных положений криптоанализа. В частности, открытый ключ не может доставляться посредством незащищенной среды. В противном случае невозможно гарантировать его подлинность. Возникает необходимость в специализированной доставке, например, курьерской. В отдельных случаях стоимость доставки может быть сравнима с затратами на производство аппаратной части.

При выпуске сертификата также могут возникнуть определенные трудности. Например, если для подтверждения подлинности открытого ключа необходимо продемонстрировать знание парного секретного ключа. К такой методике подтверждения подлинности прибегает большинство удостоверяющих центров. Для этого следует воспользоваться доказательством с нулевым разглашением, которое является вероятностным интерактивным доказательством и на практике реализуется с помощью специализированного протокола. Из теории известно, что удостоверяющий центр

примет доказательство с вероятностью не более  $1 - \frac{1}{2^\psi}$ , где  $\psi$  – число испытаний. Понятно, что  $\psi$  не может быть мало. Следовательно, задержка, связанная с выпуском сертификатов, будет зависеть от числа испытаний и исходного объема ключевого материала. Незвлекательность секретного ключа создает дополнительные проблемы.

Выпуск сертификата для каждой единицы продукции в таких массовых производствах, как, например, производство мобильных телефонов, может привести к значительной перегрузке или даже парализовать работу инфраструктуры открытых ключей. Стоимость доставки, выпуска сертификата, иных услуг инфраструктуры открытых ключей будет заложена в конечную цену устройства. Это ограничивает возможности конкурентно-ценового регулирования.

Из описания второго способа ясно, что контент, зашифрованный на ключе  $K$ , может быть расшифрован и воспроизведен только на устройстве с неизвлекаемым ключом  $K$ . Это неудобно для потребителя. Например, для прослушивания одного и того же музыкального клипа на двух различных аудиоустройствах понадобятся два различных MP3-файла. Такое неудобство может отрицательно сказаться на востребованности услуги.

В завершение отметим, что применение методов асимметричной криптографии, для которых эффективность атаки определяется вычислительной трудоемкостью решения специфических задач, не оправдано в долгосрочной перспективе [32–36].

Метод биометрической вуали свободен от обозначенных недостатков. Отпадает необходимость в инфраструктуре открытых ключей. Можно воспроизводить контент на любом устройстве потребителя без всяких ограничений. Одновременно биометрия может использоваться также в других целях, например, для разграничения доступа к устройству воспроизведения.

Отрезок времени, в течение которого ключ  $K$  сохраняется в памяти, обусловлен требованиями политики безопасности. Для метода биометрической вуали ключ сохраняется в памяти в течение ограниченного промежутка времени, необходимого для расшифрования загруженного в устройство контента. По завершении операции ключ удаляется. Такой подход имеет преимущество перед неизвлекаемыми ключами, так как позволяет воспользоваться недорогими технологическими решениями. Ведь неизвлекаемый ключ должен надежно сохраняться в памяти на протяжении всей “жизни” устройства.

Подчеркнем, что применение метода биометрической вуали не позволяет решить проблему незаконного тиражирования принципиально, но существенно ограничивает ее масштабы.

## § 9. Заключение

Метод биометрической вуали предназначен для связывания биометрических данных и криптографического ключа. Несложно выделить ключ при условии однородности образа и эталона. Высокая вычислительная трудоемкость задачи выделения ключа для  $T \neq S$  имеет теоретическое обоснование. При известном ключе возможно раскрытие эталона с помощью исчерпывающего перебора. Объем перебора определяется типом биометрии. Метод биометрической вуали применим на практике, в частности, для регулируемого распространения цифрового контента. Он позволяет существенно ограничить масштабы незаконного тиражирования.

Подавляющее большинство современных моделей мобильных телефонов и смартфонов оснащены камерами. Правдоподобно предположить, что качества оптики и разрешения существующих камер достаточно для сканирования радужной оболочки глаза. Не исключено, что для получения образа необходим специальный тип сканирующей камеры. Например, в [29] применялась сканирующая камера LG-3000 IrisAccess, работающая в длинноволновой ИК-области спектра (700–900 нм). Камера включает сертифицированный анализатор, позволяющий эффективно отсеивать

артефакты, такие, например, как фотографии радужной оболочки. Разработка подходящих камер приемлемого форм-фактора, а также способы их встраивания в мобильные устройства, относятся к интенсивно развивающейся области технологий. В ближайшем будущем логично ожидать появления пользовательских устройств, оснащенных необходимым образом.

Результаты [18,19,21] обозначили новое направление применения биометрии. Возможно, эти результаты придадут дополнительный импульс исследованиям статистических свойств других, отличных от радужной оболочки глаза, биометрических объектов.

#### СПИСОК ЛИТЕРАТУРЫ

1. *Clancy T.C., Kiyavash N., Lin D.J.* Secure Smartcard-Based Fingerprint Authentication // Proc. 2003 ACM SIGMM Workshop on Biometrics Methods and Application (WBMA'03). Berkeley, USA. November 2–8, 2003. New York: ACM, 2003. P. 45–52.
2. *Monrose F., Reiter M.K., Li Q., Wetzel S.* Cryptographic Key Generation from Voice // Proc. 2001 IEEE Sympos. on Security and Privacy (S&P'2001). Oakland, USA. May 14–16, 2001. P. 202–213.
3. *Goh A., Ngo D.C.L.* Computation of Cryptographic Keys from Face Biometrics // Communications and Multimedia Security: Advanced Techniques for Network and Data Protection (Proc. 7th IFIP-TC6 TC11 Int. Conf. on Communications and Multimedia Security (CMS'2003). Torino, Italy. October 2–3, 2003). Lecture Notes in Computer Science. V. 2828. Berlin: Springer-Verlag, 2003. P. 1–13.
4. *Hao F., Chan C.W.* Private Key Generation from On-line Handwritten Signatures // Inf. Manag. Comput. Security. 2002. V. 10. № 4. P. 159–164.
5. *Monrose F., Reiter M.K., Wetzel S.* Password Hardening Based on Keystroke Dynamics // Proc. 6th ACM Conf. on Computer and Communications Security (CCS'99). Singapore. November 1–4, 1999. New York: ACM, 1999. P. 73–82.
6. *Soutar C., Roberge D., Stoianov A., Gilroy R., Vijaya Kumar B.V.K.* Biometric Encryption // ICSA Guide to Cryptography. New York: McGraw-Hill, 1999. Ch. 22. P. 649–675.
7. *Anderson R.J.* Security Engineering: A Guide to Building Dependable Distributed Systems. Indianapolis: Wiley, 2008.
8. *Soutar C., Roberge D., Stoianov A., Gilroy R., Vijaya Kumar B.V.K.* Biometric Encryption Using Image Processing // Optical Security and Counterfeit Deterrence Techniques II (Conf. Proc.). San Jose, USA. January 28–30, 1998. Proc. SPIE. V. 3314. Bellingham, WA: SPIE, 1998. P. 178–188.
9. *Soutar C., Roberge D., Stoianov A., Gilroy R., Vijaya Kumar B.V.K.* Biometric Encryption: Enrollment and Verification Procedures // Optical Pattern Recognition IX (Conf. Proc.). Orlando, USA. April 14–15, 1998. Proc. SPIE. V. 3386. Bellingham, WA: SPIE, 1998. P. 24–35.
10. *Juels A., Sudan M.* A Fuzzy Vault Scheme // Des. Codes Cryptogr. 2006. V. 38. № 2. P. 237–257.
11. Мак-Вильямс Ф.Д., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
12. *Berlekamp E.R., McEliece R.J., van Tilborg H.C.A.* On the Inherent Intractability of Certain Coding Problems // IEEE Trans. Inform. Theory. 1978. V. 24. № 3. P. 384–386.
13. *Vardy A.* The Intractability of Computing the Minimum Distance of a Code // IEEE Trans. Inform. Theory. 1997. V. 43. № 6. P. 1757–1766.
14. *Vardy A.* Algorithmic Complexity in Coding Theory and the Minimum Distance Problem // Proc. 29th Ann. ACM Sympos. on Theory of Computing (STOC'97). El Paso, USA. May 4–6, 1997. P. 92–109.
15. *Dumer I., Micciancio D., Sudan M.* Hardness of Approximating the Minimum Distance of a Linear Code // IEEE Trans. Inform. Theory. 2003. V. 49. № 1. P. 22–37.
16. *Guruswami V., Vardy A.* Maximum-Likelihood Decoding of Reed–Solomon Codes Is NP-Hard // IEEE Trans. Inform. Theory. 2005. V. 51. № 7. P. 2249–2256.

17. *Guruswami V., Sudan M.* Improved Decoding of Reed–Solomon Codes and Algebraic Geometry Codes // IEEE Trans. Inform. Theory. 1999. V. 45. № 6. P. 1757–1767.
18. *Daugman J.G.* The Importance of Being Random: Statistical Principles of Iris Recognition // Pattern Recognition. 2003. V. 36. № 2. P. 279–291.
19. *Daugman J.G.* How Iris Recognition Works // IEEE Trans. Circ. Syst. Video Techn. 2004. V. 14. № 1. P. 21–30.
20. *Daugman J.G.* Complete Discrete 2D Gabor Transforms by Neural Networks for Image Analysis and Compression // IEEE Trans. Acoust. Speech Signal Process. 1988. V. 36. № 7. P. 1169–1179.
21. *Daugman J.G.* Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons // Proc. IEEE. 2006. V. 94. № 11. P. 1927–1935.
22. *Barg A., Krouk E., van Tilborg H.C.A.* On the Complexity of Minimum Distance Decoding of Long Linear Codes // IEEE Trans. Inform. Theory. 1999. V. 45. № 5. P. 1392–1405.
23. *Lenstra A.K., Verheul E.R.* Selecting Cryptographic Key Sizes // J. Cryptology. 2001. V. 14. № 4. P. 255–293.
24. *Lenstra A.K.* Key Lengths // Handbook of Information Security. V. II: Information Warfare; Social, Legal, and International Issues; and Security Foundations. Hoboken, N.J.: Wiley, 2006. P. 617–635.
25. Yearly Report on Algorithms and Keysizes (2009–2010). European Network of Excellence in Cryptology II (ECRYPT II), ICT-2007-216676. March, 2010. Available at <http://www.ecrypt.eu.org/documents/D.SPA.13.pdf>.
26. *Barker E., Barker W., Burr W., Polk W., Smid M.* Recommendation for Key Management. Part 1: General // NIST Special Publication 800-57. 2007. Available at [http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2\\_Mar08-2007.pdf](http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf).
27. *Чмора А.Л., Уривский А.В.* Биометрическая система аутентификации, способ представления и выделения криптографического ключа на основе биометрических данных: Патент 2004114316. Россия, 2004.
28. *Chmora A., Ourivski A.* Method and Apparatus for Generating Cryptographic Key Using Biometric Data: US Pat. Appl. № 20100014655. January 21, 2010.
29. *Hao F., Anderson R., Daugman J.G.* Combining Crypto with Biometrics Effectively // IEEE Trans. Comput. 2006. V. 55. № 9. P. 1081–1088.
30. *Blaze M., Diffie W., Rivest R.L., Schneier B., Shimomura T., Thompson E., Wiener M.* Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security. Report by an ad hoc Group of Cryptographers and Computer Scientists. January 1996.
31. *Bertoni G., Breveglieri L., Fragneto P., Macchetti M., Marchesin S.* Efficient Software Implementation of AES on 32-bit Platforms // Proc. 4th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES'2002). Redwood Shores, CA, USA. August 13–15, 2002. Lecture Notes in Computer Science. V. 2523. Berlin: Springer-Verlag, 2003. P. 159–171.
32. *Ekert A., Jozsa R.* Quantum Computation and Shor's Factoring Algorithm // Rev. Modern Phys. 1996. V. 68. № 3. P. 733–753.
33. *Shor P.W.* Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM J. Comput. 1997. V. 26. № 5. P. 1484–1509.
34. *Vandersypen L.M.K., Steffen M., Breyta G., Yannoni C.S., Sherwood M., Chuang I.L.* Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance // Nature. 2001. № 414. P. 883–887.
35. *Beauregard S.* Circuit for Shor's Algorithm Using  $2n + 3$  Qubits // Quantum Inf. Comput. 2003. V. 3. № 2. P. 175–185.
36. *Hanneke D., Home J.P., Jost J.D., Amini J.M., Leibfried D., Wineland D.J.* Realization of a Programmable Two-Qubit Quantum Processor // Nature Physics. 2010. V. 6. № 1. P. 13–16.

Чмора Андрей Львович  
 ОАО «Инфотекс» (Информационные технологии  
 и коммуникационные системы)  
 chmora@infotecs.ru

Поступила в редакцию  
 07.04.2010  
 После переработки  
 06.12.2010