УДК 004.056.5

А.А. КУЗНЕЦОВ, д-р техн. наук, Р.В. СЕРГИЕНКО, канд. техн. наук, А.А. УВАРОВА

НЕЧЕТКИЙ ЭКСТРАКТОР НА ПОМЕХОУСТОЙЧИВЫХ КОДАХ ДЛЯ БИОМЕТРИЧЕСКОЙ КРИПТОГРАФИИ

Введение

Важным направлением современных исследований в области киберзащиты являются биометрические методы аутентификации личности [1 – 12]. Они широко используются в различных приложениях: криминалистике, электронной коммерции, защите авторского права, электронном документообороте и пр.

В последние годы интерес к биометрическим методам значительно расширился. От традиционных биометрических систем, основанных на сравнении полученных биометрических образов с хранимыми эталонными копиями, современные технологии перешли к формированию криптографических ключей «на лету». В этом случае биометрические данные уже не нуждаются в хранении, передаче, сложных и дорогостоящих средствах защиты и т.д., исключается возможность их преднамеренной и/или случайной компрометации. Все процедуры верификации, идентификации и аутентификации выполняются по деперсонализированным криптографическим ключам (паролям, кодам доступа, пин-кодам), а уникальные биометрические персональные данные личности остаются в безопасности. Формируемые деперсонализированные ключевые последовательности будем называть в дальнейшем биометрическими ключами.

Следующим этапом в развитии подобных технологий будет построение полноценных биометрических криптографических систем, в которых биометрические данные личности должны использоваться как источник уникальных секретных параметров. При этом пользователю не нужно будет запоминать криптографические ключи (пароли) и/или использовать дополнительные устройства их хранения, передачи и пр. Биометрическая криптосистема в любое время и в любом месте инициализируется посредством извлечения «на лету» нужных параметров из предоставленных биометрических образов (с возможными ошибками, стираниями и пр.) без компрометации этих образов. При этом необходимо обеспечить максимальный набор услуг и гарантий безопасности, учитывающих особенности построения биометрических криптосистем.

В данной работе рассматриваются методы формирования криптографических ключей из биометрических образов[1] с использованием нечетких экстракторов [3, 4].

Традиционно нечеткие экстракторы, как и предшествовавшие им нечеткие контейнеры [2], строятся с использованием методов помехоустойчивого кодирования. На начальном этапе биометрические данные в некотором смысле «объединяются» с элементами помехоустойчивых кодов (например, с кодовыми словами или синдромными последовательностями). Для нечетких экстракторов дополнительно формируется открытая вспомогательная строка (helper string), которая «помогает» в извлечении секретного параметра по нечетко заданной биометрии. На этапе непосредственного использования применяется помехоустойчивое декодирование, которое устраняет возможную неопределенность (вызванную искажениями, стираниями и пр.) в предоставленных пользователем биометрических образах. Если различия в наборах характеристик невелики (не превышают исправляющей способности кодов), тогда нечеткие экстракторы (хранилища) позволяют однозначно восстановить секретный параметр (биометрический ключ).

[1] Под биометрическими образами (данными) здесь и далее понимаются наборы биометрических характеристик, представимых в виде бинарных векторов, которые можно сравнивать в метрике Хемминга. Предполагается, что различные наборы характеристик одного и того же пользователя отличаются друг от друга не более, чем на 25 % (этот порог соответствует предельным корректирующим возможностям помехоустойчивых кодов).

В данной работе предлагается новая схема нечеткого экстрактора, в основе которой лежит кодовая криптосистема Мак-Элиса [13]. Показано, что новая конструкция позволяет формировать криптографические пароли из биометрических образов даже без использования несекретных helper string. При использовании helper string значительно возрастает доля корректируемых искажений биометрических образов. Кроме того, предлагаемая конструкция относится к классу постквантовых методов защиты информации, т.е. ожидается ее безопасное использование даже в условиях применения универсальных квантовых компьютеров для решения задач криптографического анализа.

Нечеткие хранилища и нечеткие экстракторы

В [1] рассмотрено формирование секретного ключа с использованием биометрии, упрощенная схема которого приведена на рис. 1.

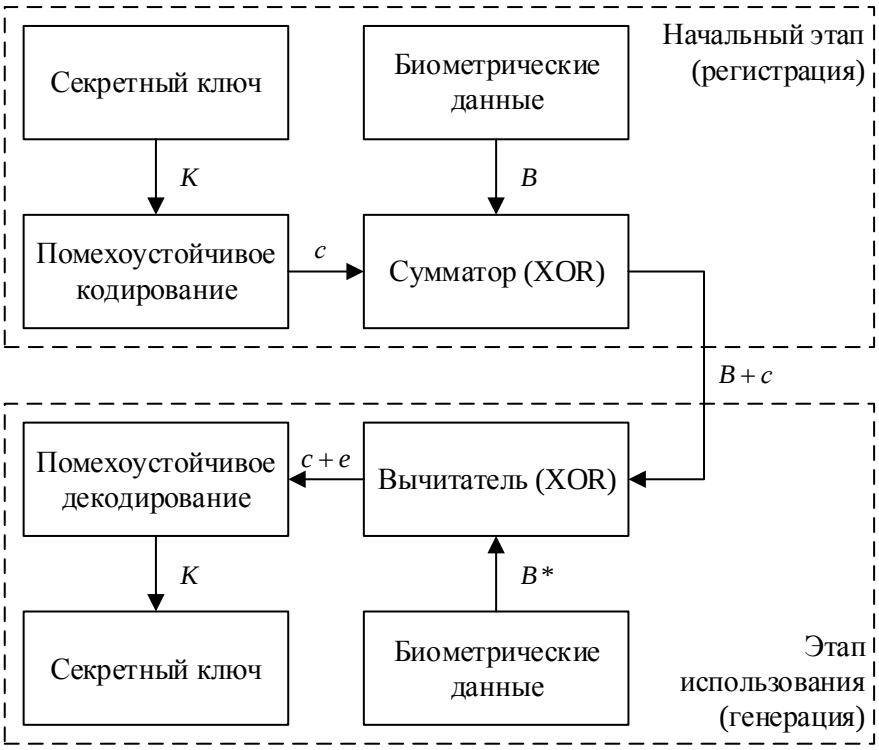

Рис. 1. Схема формирования биометрического ключа

На начальном этапе формируется секретный параметр (ключ) K, который кодируется помехоустойчивым кодом. К полученному кодовому слову c прибавляются биометрические данные пользователя B. Полученный «носитель» $B+c$ фактически является зашумленным биометрией секретным ключом. Если на этапе использования будут предоставлены биометрические данные B^*, близкие к исходным $B^* \approx B$, тогда, после их вычитания, декодирование позволит восстановить секретный ключ. Действительно, после вычитания получим:

$$(B+c)-B^*=c+e,$$

где $e=B-B^*$ интерпретируется как вектор ошибок.

Если вес Хемминга вектора e (число ненулевых его компонент) не превышает исправляющей способности помехоустойчивого кода t, тогда декодирование вектора $(B+c)-B^*$ позволит найти вектор c, вектор e и, как следствие, ключевой параметр K.

Очевидно, что криптографические свойства схемы [1] зависят как от выбранного помехоустойчивого кода, так и от способа формирования биометрических данных. Секретный параметр K в закодированном виде содержится в «носителе» $B+c$ и, очевидно, возможны статистические атаки, восстанавливающие кодовое слово c и секретный ключ K.

Схема нечеткого хранилища впервые предложена в работе [2]. В ее основе также лежит использование помехоустойчивых кодов. Секретный параметр «прячется» в закодированном наборе данных, предоставленных пользователем. Любой пользователь сможет извлечь секретный параметр только если его набор будет близок к исходному набору, а небольшие различия будут исправлены в процессе помехоустойчивого декодирования. Статистический анализ нечеткого хранилища вероятно может привести к возможной атаке на хранящийся секретный ключ.

Дальнейшее развитие технологии биометрических ключей получило в работах [3 – 12] и др. В частности, в основополагающих работах [3, 4] предложены так называемые нечеткие экстракторы, конструкции которых очень близки к схемам формирования ключей из [1]. Основными являются две конструкции [3, 4]:

- на основе кодовых слов (рис. 2);
- на основе синдромов (рис. 3).

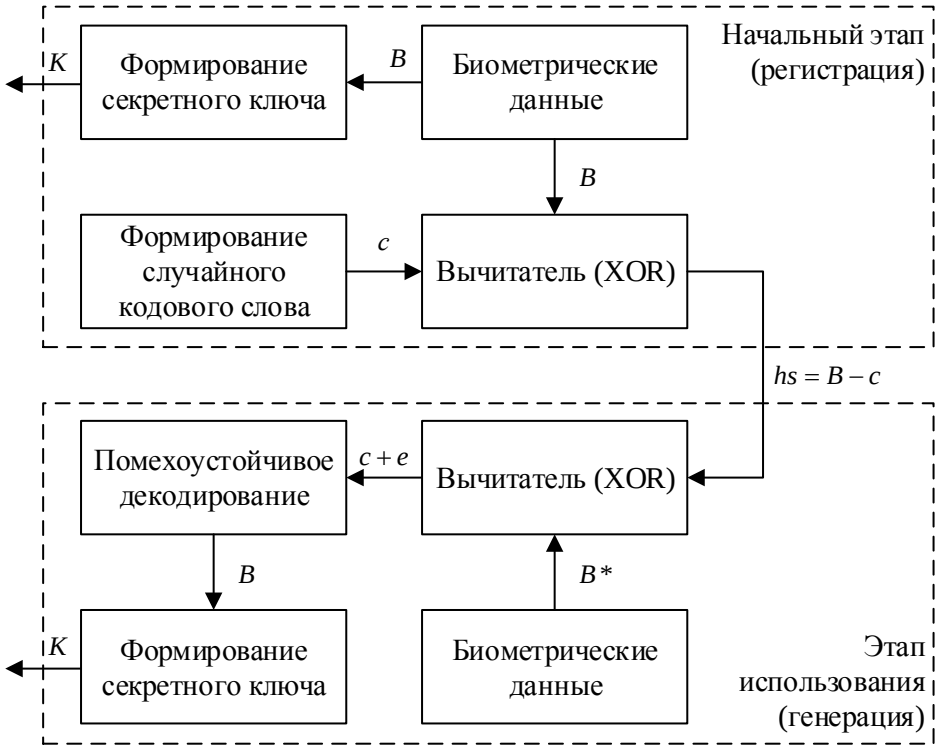

Рис. 2. Схема нечеткого экстрактора на основе кодовоых слов

Пусть задан помехоустойчивых блоковый $(n, k, d = 2t+1)$ код с исправляющей способностью t ошибок. Предполагается, что наличие биометрических данных B позволяет сформировать секретный ключ K и некоторую helper string hs (для этого используются различные приемы и техники, например Secure Sketches [3, 4]).

В первой конструкции (на основе кодовых слов, см. рис. 2) на начальном этапе (регистрации биометрического ключа) формируется случайное кодовое слово c. Открытая вспомогательная строка hs формируется посредством вычитания из биометрических данных B слова c:

$$hs = B - c,$$

причем по этой открытой строке в последствии можно восстановить секретный ключ K.

Действительно, на этапе использования пользователь предоставляет биометрические данные B^*, из которых отнимается подсказка hs. Если $B^* \approx B$ тогда имеем

$$B^* - hs = B^* - (B - c) = c + e,$$

где $e = B^* - B$, и если вес Хемминга вектора e не превышает t, тогда декодирование вектора $B^* - hs$ позволит найти вектор c, вектор e и, как следствие, биометрические данные B:

$$B = c + hs.$$

Правильное восстановление биометрических данных B позволяет сформировать секретный ключ K (как и на этапе регистрации).

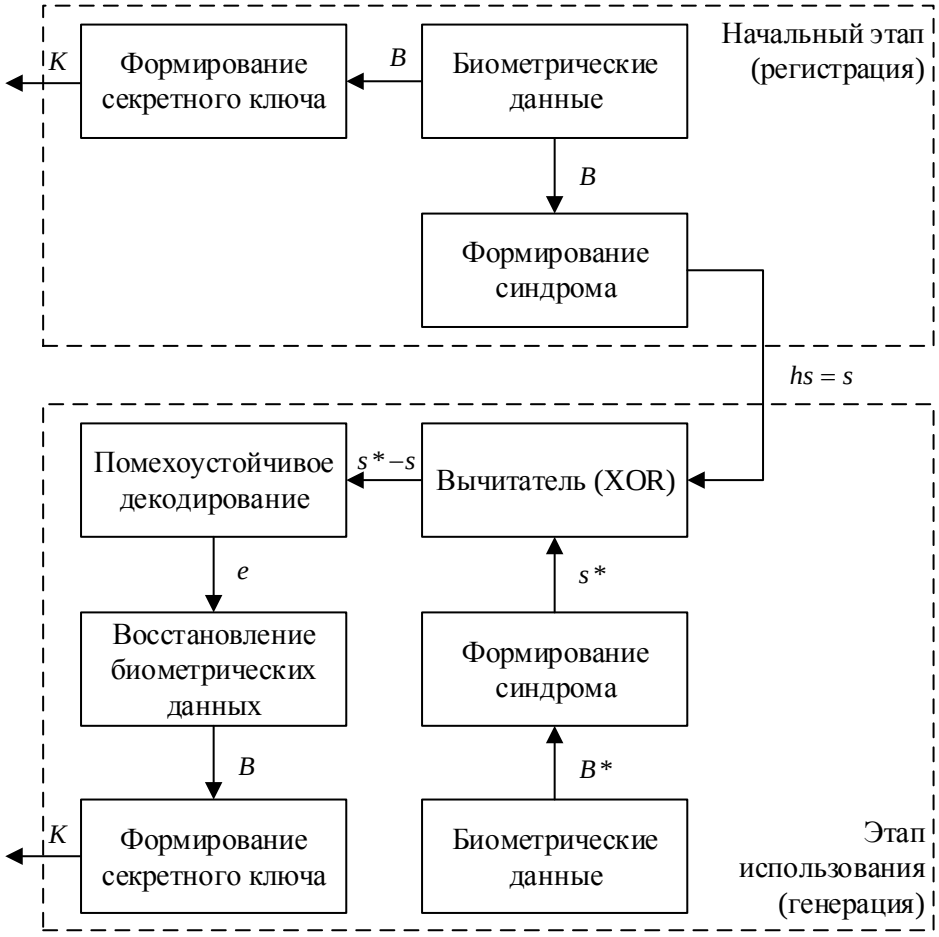

Рис. 3. Схема нечеткого экстрактора на основе синдромов

Вторая схема (см. рис. 3) оперирует синдромными последовательностями s, которые зависят исключительно от вектора ошибок e. Например, для линейных блоковых кодов, заданных проверочной матрицей H, для любого кодового слова c справедливы равенства [14, 15]:

$$c \cdot H^T = 0,\ s = (c + e) \cdot H^T = e \cdot H^T.$$

На начальном этапе с использованием B формируется синдромная последовательность s, которая выступает в качестве открытых вспомогательных данных. На этапе использования пользователь предъявляет биометрические данные B^*, по которым вычисляется синдромная последовательность s^*. Если $B^* \approx B$, тогда наличие подсказки $hs = s$ и синдрома s^* позволяет восстановить B и сформировать секретный ключ K.

Действительно, если, например, $s = B \cdot H^T$ и $s^* = B^* \cdot H^T$, тогда

$$s^* - s = e \cdot H^T,$$

где $e = B^* - B$, и если вес Хемминга вектора e не превышает t, тогда синдромное декодирование вектора $s^* - s$ позволит найти вектор e.

Правильное восстановление биометрических данных $B = B^* - e$ позволяет сформировать секретный ключ K (как и на этапе регистрации).

Очевидно, что схемы на рис. 1 и 2 для двоичного случая (сложение и вычитание реализуются операцией XOR) практически совпадают. Основное отличие состоит в том, что на рис. 1 секретный ключ формируется случайным образом, а затем кодируется помехоустойчивым кодом. На рис. 2 секретный ключ формируется из биометрических данных B, которые однозначно должны быть восстановлены в случае представления пользователем данных $B^* \approx B$. Однако в обеих схемах используется общий подход, состоящий в «подмешивании» биометрических данных B к кодовому слову c (случайно сформированному или как закодированному ключу K). Это, на наш взгляд, несет основную угрозу использования подобных биометрических ключей. Если в открытом виде передаются, хранятся и/или обрабатываются биометрические данные (даже с подмешанными к ним кодовыми словами, синдромами и пр.), следует ожидать статистических атак, направленных на восстановление кодовых слов c, биометрических данных B и ключей K.

В данной работе предлагается новая схема нечеткого экстрактора, в которой биометрические данные не хранятся и не передаются ни в каком виде. Наша схема использует кодовую криптосистему Мак-Элиса в интерпретации Code-Based Electronic Digital Signature из работы [16].

Предлагаемая схема нечеткого экстрактора

В основе нашего предложения лежит использование кодовой криптосистемы Мак-Элиса [13].

А. Кодовая криптосистема Мак-Элиса

Кодовая криптосистема Мак-Элиса предложена в 1978 году [13] и за 40 лет существования не обнаружила существенных уязвимостей. В случае использования кодов Гоппы [17] с достаточной длиной и кодовым расстоянием считается надежным кандидатом на постквантовое применение, т.е. предполагается ее безопасное использование даже при использовании полномасштабных универсальных квантовых компьютеров для решения задач криптографического анализа [18, 19].

Открытым ключом в схеме Мак-Элиса является матрица

$$G_X = X \cdot G \cdot P \cdot D, \tag{1}$$

где G – порождающая матрица алгебраического $(n, k, d = 2t+1)$ кода над $GF(q)$ (в оригинальной статье [13] предлагалось использовать двоичный код Гоппы [17]), X – невырожденная $k \times k$ матрица с элементами из $GF(q)$, P и D – перестановочная и диагональная $n \times n$ матрицы (для двоичных кодов используется только матрица P).

Матрицы X, P и D в (1) являются секретным ключом, который маскирует используемый алгебраический блоковый код под случайный код (код общего положения), т.е. открытый ключ G_X представляется злоумышленнику как случайно сформированная порождающая матрица некоторого линейного кода, для которого неизвестен алгоритм быстрого декодирования. Напротив, уполномоченный пользователь, знающий секретный ключ (матрицы X, P и D), может снять действие маскирующих матриц и воспользоваться быстрым алгоритмом декодирования алгебраического кода с порождающей матрицей G.

Криптограмма представляет собой вектор длины n, который вычисляется по правилу

$$c_X^* = I \cdot G_X + e, \tag{2}$$

где вектор

$$c_X = I \cdot G_X$$

является кодовым словом замаскированного кода, т.е. c_X принадлежит $(n,k,d=2t+1)$ коду с порождающей матрицей G_X, I – k-разрядный информационный вектор над $GF(q)$, вектор e – секретный вектор ошибок веса t.

Злоумышленнику необходимо декодировать c_X^*, используя известную ему порождающую матрицу G_X. Однако декодирование случайного кода (при соответствующих параметрах n,k,q и $d=2t+1$) вычислительно недостижимо. Не зная матрицы X, P и D злоумышленник не может восстановить матрицу G и воспользоваться алгоритмом декодирования полиномиальной сложности. Для уполномоченного пользователя (знающего секретный ключ) декодирование – полиномиально разрешимая задача. Действительно, легитимный пользователь, получив вектор c_X^*, строит вектор

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}. \quad (3)$$

Далее, используя алгоритм полиномиальной сложности, он декодирует вектор $\bar{c}^* = I' \cdot G + e'$, т.е. находит I'. Затем вычисляет k-разрядный информационный вектор

$$I = I' X^{-1}. \quad (4)$$

Дополнительным секретным параметром, который можно использовать в случае применения кодов Гоппы, является многочлен Гоппы $G(x)$ [13].

В. Новая схема нечеткого экстрактора на помехоустойчивых кодах

Предлагаемая схема нечеткого экстрактора позволяет формировать криптографические ключи даже без использования несекретных helper string. При использовании helper string значительно возрастает доля корректируемых искажений биометрических образов.

Упрощенная схема предлагаемого нечеткого экстрактора приведена на рис. 4.

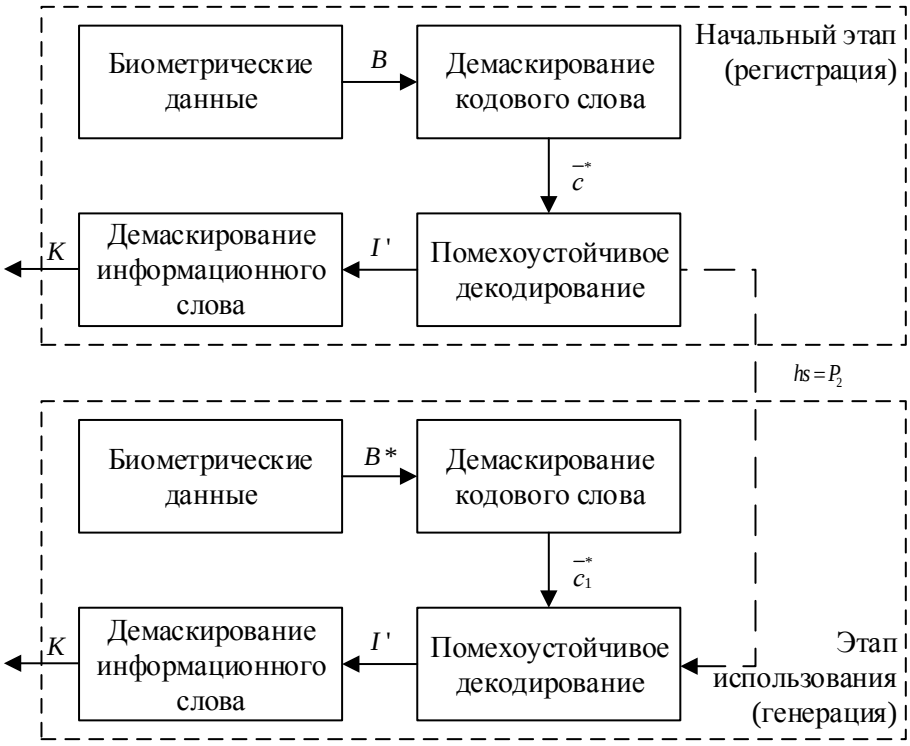

Рис. 4. Предлагаемая схема нечеткого экстрактора (прерывистая линия соответствует возможному использованию helper string)

На начальном этапе биометрические данные[2] B интерпретируются как кодовое слово (2) замаскированного кода в криптосистеме Мак-Элиса. В соответствии с (3) производится его демаскирование, полученный вектор $\overline{c}^*$ декодируется. Из декодированного кодового слова извлекается вектор I', который также демаскируется в соответствии с (4). Полученная информационная последовательность I интерпретируется как секретный биометрический ключ K. В простейшем случае $K = I$, хотя возможна и более сложная конструкция генерации K из I, например посредством однонаправленного хеширования: $K = h(I \| i)$, где $x \| y$ – операция конкатенации (присоединения) строк x и y; i – дополнительные (служебные) данные, которые используются для вычисления секретного ключа.

На этапе использования пользователь предъявляет биометрические данные B^*, которые, как и на этапе регистрации, интерпретируются как кодовое слово (2) замаскированного кода в криптосистеме Мак-Элиса. В соответствии с (3) производится его демаскирование, полученный вектор (обозначим его $\overline{c}_1^*$) декодируется. Если $B^* \approx B$ и, в нашей интерпретации,

$$B = I \cdot G_X + e \quad \text{и} \quad B^* = I \cdot G_X + e^*, \tag{5}$$

где e и e^* – два различных вектора с весом Хемминга меньше t, тогда декодирование векторов

$$\overline{c}^* = (I \cdot G_X + e) \cdot D^{-1} \cdot P^{-1} = I' \cdot G + e \cdot D^{-1} \cdot P^{-1}$$

и

$$\overline{c}_1^* = (I \cdot G_X + e^*) \cdot D^{-1} \cdot P^{-1} = I' \cdot G + e^* \cdot D^{-1} \cdot P^{-1}$$

позволит восстановить один и тот же вектор I'.

После демаскировании вектора I' по правилу (4) формируется секретный ключ K (как и на этапе регистрации).

В основе нашего метода лежит предположение (5), которое по сути сводится к наличию у всех биометрических характеристик, принадлежащих одному и тому же пользователю, некоторой общей информации (энтропии), которую условно можно задать вектором I. Эта информация в закодированном виде искажается в процессе обработки биометрических образов (использование различных биометрических датчиков, влияние помех, стираний и пр.). Если предположить, что биометрические образы искажаются ошибками, вес Хемминга которых не превосходит исправляющей способности t, тогда во всех случаях использования секретный ключ будет восстановлен верно. Для снижения влияния случайных ошибок на этапе регистрации следует сформировать наиболее достоверный набор биометрических характеристик, например посредством многократного формирования с усреднением полученного результата.

Эффективность использования предлагаемого нечеткого экстрактора, как и других рассмотренных выше методов, зависит от характеристик используемого помехоустойчивого кода. Фактически False Rejection Rate (FRR) определяется вероятностью ошибочного декодирования (для случая $B^* \approx B$). Однако наше предположение (5) выглядит более естественным, в предлагаемом экстракторе исправляются различные искажения одного и того же кодового слова, содержащего биометрическую энтропию. В схемах [1, 3, 4] исправляются различия биометрических образов одного и того же пользователя, т.е. основное предположение, лежащее в основе этих конструкций, имеет вид $|B - B^*| = e$, где вес Хемминга вектора e

[2] Предполагается, что на этапе регистрации формируется наиболее достоверный набор биометрических характеристик, представленных в виде бинарных векторов

должен быть меньше t. Если учесть возможность разнонаправленного искажения биометрических образов $B-B^*$, тогда наш экстрактор интуитивно представляется более надежным.

Следует отметить, что в схеме на рис. 4 может вовсе не использоваться helper string, т.е. наш экстрактор может работать «вслепую». Из каждого предоставленного биометрического образа будут извлечены ключевые данные и, при выполнении (5), восстановленные ключи будут совпадать.

Тем не менее дополнительное использование helper string существенно снижает FRR.

Запишем матрицу G в виде «объединения» двух подматриц – квадратной матрицы G_1 размерности $k \times k$ и прямоугольной матрицы G_2 размерности $k \times (n-k)$:

$$G = G_1 \| G_2 . \tag{6}$$

Тогда слово $\bar{c} = I' \cdot G$ можем записать в виде

$$\bar{c} = P_1 \| P_2 , \text{ где } P_1 = I' \cdot G_1 , \; P_2 = I' \cdot G_2 .$$

Используя последние тождества найдем:

$$P_2 = P_1 \cdot G_1^{-1} \cdot G_2 , \tag{7}$$

где матрица G_1^{-1} является обратной[3] к матрице G_1.

На рис. 4 прерывистая линия соответствует возможному использованию P_2 в качестве helper string (на этапе использования при декодировании $\bar{c}_1^*$). Это позволяет значительно снизить действие ошибок и повысить, таким образом, вероятность правильного восстановления вектора I' и секретного ключа K (т.е. снизить FRR). Действительно, если ошибки (ненулевые элементы вектора e) распределены равномерно по всему слову $\bar{c}^* = I' \cdot G + e'$, тогда, имея неискаженную часть P_2 кодового слова $I' \cdot G$, можно «проигнорировать» все ошибки, приходящиеся на «вторую» часть слова. Это эквивалентно повышению исправляющей способности кода соответственно длине вектора P_2. Поясним это следующими рассуждениями.

Пусть ошибки (ненулевые элементы вектора e) происходят случайно, равновероятно и независимо друг от друга. Обозначим символом p – вероятность искажения одного символа кодового слова. Тогда вероятность искажения m символов кодового слова длины n:

$$P(m) = C_n^m p^m (1-p)^{n-m},$$

где $C_n^m = \dfrac{n!}{m!(n-m)!}$ – биномиальный коэффициент.

Вероятность ошибки декодирования (соответствует FRR в нашей модели без применения helper string) при использовании $(n, k, d = 2t+1)$ кода запишется в виде

$$FRR = 1 - \sum_{i=0}^{t} P(i) = 1 - \sum_{i=0}^{t} C_n^i p^i (1-p)^{n-i} . \tag{8}$$

При использовании helper string ошибки нужно исправить только на позициях вектора P_1, и вероятность ошибки декодирования (при аналогичных рассуждениях) примет вид

[3] Для обратимости матрицы G_1 необходимо правильно реализовать представление (6): это не «объединение» первых (любых) k столбцов матрицы G, а псевдослучайный выбор таких k столбцов из G, которые образуют невырожденную квадратную матрицу G_1.

$$FRR^* = 1 - \sum_{i=0}^{t} C_k^i p^i (1-p)^{k-i} . \quad (9)$$

На рис. 5 приведены расчетные зависимости FRR для некоторых (*n, k, d*) параметров двоичных кодов БЧХ: *а* – (127, 64, 21); *б* – (255, 115, 43); *в* – (512, 211, 83).

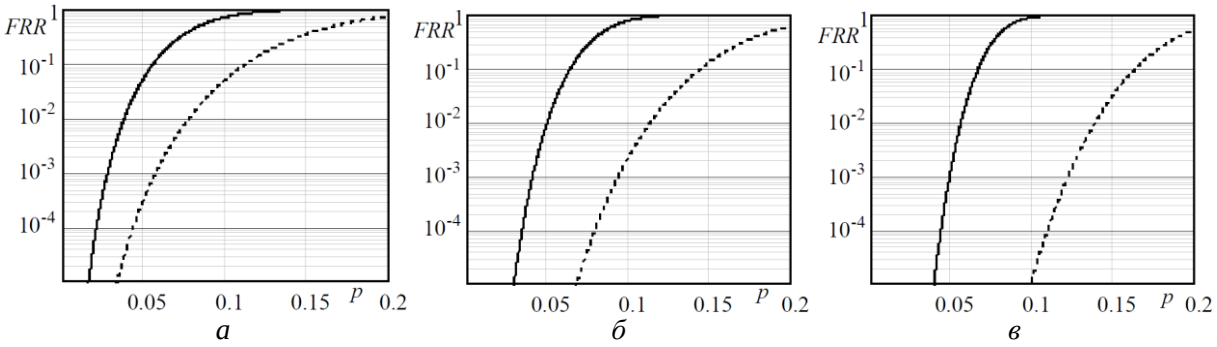

Рис. 5. Расчетные зависимости FRR (сплошная линия – без helper string; прерывистая линия – с helper string)

Как следует из приведенных зависимостей, при выборе соответствующих (*n, k, d*) параметров FRR может быть очень низкой. Например, при формировании 64-битного ключа с использованием двоичного (127, 64, 21)-кода и $p = 0,05$ значение FRR для экстрактора без helper string не превосходит 10^{-1}. Использование helper string снижает FRR на два порядка. Увеличение длины и исправляющей способности кода приводит к снижению FRR. Например, для (512, 211, 83)-кода с даже для $p = 0,15$ использование helper string позволяет сформировать 211 битный ключ с FAR не более 10^{-1}.

Следует отметить, что другая важная характеристика биометрических паролей False Acceptance Rate (FAR), характеризующая вероятность ошибочного формирования секретного ключа неуполномоченным пользователем, возрастает при увеличении исправляющей способности t кода. При значительном увеличении t (за счет увеличения избыточности P_2) экстрактор сможет извлекать один и тот же ключ для любых предоставленных биометрических данных, т.е. для $B^* \neq B$. Например, если использовать двоичный код с параметрами (511, 112, 239) с 399-битной подсказкой $hs = P_2$, тогда даже при искажении всех 112 бит вектора P_1, экстрактор их исправит ($t = 119$) и однозначно восстановит вектор I и секретный ключ K. Другими словами, любой пользователь, предоставивший произвольный набор B^*, сможет правильно восстановить ключ K. С этой точки зрения при выборе (*n, k, d*) параметров кода следует выбирать компромиссное решение между ожидаемыми значениями FRR и FAR. Если предположить, что $k < \frac{n}{2}$ и все пользователи обладают равноудаленными друг от друга биометрическими данными, тогда FAR (при использовании helper string) можно условно оценить следующим выражением:

$$FAR^* = \begin{cases} q^{-k+t}, & k > t; \\ 1, & k \le t, \end{cases} \quad (10)$$

где q – мощность алфавита символов, над которым построен помехоустойчивых код (для двоичного кода $q = 2$).

Действительно, в предложенном экстракторе в качестве секретного ключа K используется вектор I (или функция от этого вектора) длины k кодовых символов. При равноудаленных кодовых словах (биометрических образах) и равновероятном их выборе вероятность

совпадения ключей для разных пользователей равна q^{-k}. Нечеткий экстрактор основан на помехоустойчивом декодировании и, в случае использования helper string, все t ошибок могут быть исправлены на блоке P_1 длиной k кодовых символов, т.е., если $k > t$ вероятность совпадения секретных ключей для различных равновероятно выбранных биометрических образов будет равна q^{-k+t}. Для $k \le t$ исправляющая способность кода позволяет полностью подобрать нужный вектор для любого биометрического набора, т.е. «пропуск цели» является достоверным событием. Если helper string не используется, тогда на каждые k кодовых символов приходится в среднем $\frac{t}{n}$ исправляемых ошибок и FAR можно оценить как $q^{-k+\frac{t}{n}k}$.

В заключение отметим, что все приведенные рассуждения, соотношения и расчетные значения приведены для «идеальных» условий, когда наборы биометрических характеристик формируются в виде бинарных векторов со случайными, равновероятными (при $p < 0,5$) и независимыми ошибками. В реальных условиях характер ошибок может значительно отличаться. Необходимо проводить дальнейшие исследования, в том числе экспериментального характера для обоснования практических рекомендаций по непосредственному использованию предложенного нечеткого экстрактора.

Выводы

Предложен нечеткий экстрактор, основанный на кодовой криптосистеме Мак-Элиса. Наше предложение, с одной стороны, использует сильные стороны кодовой криптосистемы: криптографическую стойкость, основанную на проблеме синдромного декодирования; устойчивость к квантовым методам криптоанализа; относительно высокую скорость преобразования (по сравнению с другими криптосистемами с открытым ключом). С другой стороны, наш экстрактор посредством подбора нужных (*n, k, d*) параметров помехоустойчивого кода позволяет обеспечить сколь угодно малые FRR (при условии выполнения ряда предположений о характере ошибок). Использование подсказок (helper string) значительно снижает FRR, однако с увеличением исправляющей способности кода это может увеличить FAR за счет неправильного «исправления» биометрических признаков. Выбор компромиссного решения по параметрам кода с учетом характеристики возникающих ошибок, экспериментальные исследования FRR и FAR являются перспективными направлениями дальнейшей работы.

Список литературы:

1. Hao F., Anderson R., Daugman J. Combining cryptography with biometrics effectively: Technical Report UCAM-CL-TR-640. – Cambridge: University of Cambridge Computer Laboratory, 2005. – 17 p.
2. A. Juels, M. Sudan. A fuzzy vault scheme // Des. Codes Cryptography. – 2006. – Vol. 38, no. 2. – P. 237-257..
3. Y. Dodis, R. Ostrovsky, L. Reyzin, A. D. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data // SIAM J. Comput. – 2008. – Vol. 38, no. 1. – P. 97-139,
4. Yevgeniy Dodis, Leonid Reyzin, Adam Smith. Fuzzy Extractors. A Brief Survey of Results from 2004 to 2006. [On-line]. Internet: http://www.cs.bu.edu/~reyzin/papers/fuzzysurvey.pdf
5. H. Kang, Y. Hori, T. Katashita, M. Hagiwara and K. Iwamura. Cryptographie key generation from PUF data using efficient fuzzy extractors // 16th International Conference on Advanced Communication Technology, Pyeongchang, 2014. – P. 23-26.
6. N. Li, F. Guo, Y. Mu, W. Susilo and S. Nepal. Fuzzy Extractors for Biometric Identification // IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, 2017. – P. 667-677.
7. Y. Wen and Y. Lao. Efficient fuzzy extractor implementations for PUF based authentication // 12th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, 2017. – P. 119-125.
8. T. Kaur and M. Kaur. Cryptographic key generation from multimodal template using fuzzy extractor // Tenth International Conference on Contemporary Computing (IC3), Noida, 2017. – P. 1-6.
9. N. K. Gupta and M. Kaur. A robust and secure multitrait based fuzzy extractor // 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, 2017 – P. 1-6.
10. C. Huth, D. Becker, J. Guajardo, P. Duplys and T. Güneysu. LWE-based lossless computational fuzzy extractor for the Internet of Things // IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, 2017. – P. 154-154.
11. C. Huth, D. Becker, J. G. Merchan, P. Duplys and T. Güneysu. Securing Systems With Indispensable Entropy: LWE-Based Lossless Computational Fuzzy Extractor for the Internet of Things // IEEE Access. – 2017. – Vol. 5, P. 11909-11926, 2017.
12. A. Schaller, T. Stanko, B. Škorić and S. Katzenbeisser. Eliminating Leakage in Reverse Fuzzy Extractors // IEEE Transactions on Information Forensics and Security. – 2018. – Vol. 13, no. 4. – P. 954-964

13. McEliece R. J. A public-key cryptosystem based on algebraic coding theory // DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978. – P. 114-116.

14. Clark G.C., Cain J.B. Error-Correction Coding for Digital Communications // Springer, 1981. – 432 p.

15. Blahut R. E. Theory and Practice of Error Control Codes. – Addison Wesley Publishing Company, Inc., Reading, Massachusetts, 1983, 1983 – 500 p.

16. A. Kuznetsov, A. Pushkar'ov, N. Kiyan and T. Kuznetsova. Code-based electronic digital signature // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018. – P. 331-336.

17. V.D. Goppa. A New Class of Linear Correcting Codes // Problems Inform. Transmission, 6: 3 (1970), 207-212.

18. D. Bernstein, J. Buchmann and E.Dahmen. Post-Quantum Cryptography. – Springer-Verlag, Berlin-Heidleberg, 2009. – 245 p.

Харьковский национальный
университет имени В.Н. Каразина;
Академия национальной армии
имени гетмана Петра Сагайдачного;
Государственное конструкторское
бюро «Южное», Днепр

Поступила в редколлегию 07.11.2018