УДК 681.322.067

С.М. Гончаров, А.А. Суховей

Алгоритм формирования криптографического ключа на основе особых точек отпечатка пальца

Предложен алгоритм формирования криптографического ключа на основе особых точек отпечатка пальца. Алгоритм разделен на блоки, в которых представлены основные этапы обработки данных. Описаны процедуры формирования последовательностей при регистрации пользователя в системе и последующих этапах генерации криптографического ключа.

Ключевые слова: отпечаток пальца, особые точки, криптография, нечеткие данные, генерация ключа, биометрический ключ, папиллярные линии, уникальная последовательность.

Биометрические технологии в настоящее время достаточно быстро развиваются, что связано с повышением производительности современных информационных платформ и всеобщей информатизацией общества. На стыке биометрии и криптографии сформировалось научное направление, названное «биокриптография».

Одним из основных направлений современной биокриптографии являются исследования в области применения биометрических данных в криптографических приложениях. Для этого ключевым моментом является наличие алгоритмов выработки уникальных последовательностей пользователей на основе нечетких биометрических данных.

Такой подход позволяет применять хеш-функции к биометрическим последовательностям, которые могут быть использованы в качестве ключей для криптографических алгоритмов либо материала для генерации таких ключей.

Авторами разработан алгоритм генерации ключевой последовательности для шифрования с использованием биометрических данных на основе отпечатков пальцев, который содержит 4 основных блока:

1. Блок предварительной обработки отпечатка пальца.
2. Генерация биометрической последовательности.
3. Блок Fuzzy Extractor.
4. Генерация криптографического ключа на основе битовой последовательности.

Блок предварительной обработки отпечатка пальца

Выделение особых точек отпечатка пальца и его центра невозможно без предварительной обработки изображения, поскольку исходный материал является нечетким и содержит различные шумы, вызывающие ошибки в дальнейших вычислениях [1].

Предварительная обработка отпечатка пальца сводится к преобразованию полученного со сканера изображения в бинарную матрицу с толщиной папиллярного узора в 1 пиксель.

Для решения данной задачи на первом этапе производится сглаживающая фильтрация исходного изображения.

Пусть T – полутоновое изображение размера $n \times m$; r – размер матрицы фильтра, $W(i,j) = 1/r^2; i,j \in \{0,r\}$ – фильтрующая матрица, а $t \in T$ – массив размера $r \times r$, подвергающийся фильтрации, с центральной точкой $T(i,j)$, тогда:

$$T(i,j) = \sum_{u=0}^{r} \sum_{v=0}^{r} W(u,v) * t(u,v), \quad (1)$$

где $0 \le i \le n, 0 \le j \le m$.

Полученное изображение бинаризуется относительно заданного порога. Для этого вся матрица делится на блоки размером $H \times H$. В каждом блоке рассчитывается математическое ожидание, относительно которого все точки блока преобразуются в 1 или 0.

Проведение дальнейших преобразований предполагает получение изображения с толщиной линий папиллярного узора в 1 пиксель. Для решения этой задачи выбран алгоритм скелетизации изображения Зонга–Суня.

На выходе блока предварительной обработки отпечатка пальца формируется изображение с толщиной линий, равной одному пикселю.

Генерация биометрической последовательности

Блок генерации биометрической последовательности решает задачу преобразования входного набора биометрических данных в битовую последовательность, используемую далее для формирования криптографического ключа.

Авторами предлагается использование *n*, *t*-пороговой схемы Шамира для преобразования особых точек отпечатка пальца в биометрическую последовательность.

Для решения этой задачи вводится новая система координат с центром в точке O (центр папиллярного узора), относительно которой далее производятся вычисления координат особых точек.

Этапы блока в процедуре регистрации пользователя:

1. Вычислим координаты множества особых точек $D=\{d_{xi},d_{yi}\}$ предварительно обработанного изображения отпечатка пальца. Координаты рассматриваются как элементы поля $GF(p)$, где p – простое число, задающее конечное поле $GF(p)$.

2. Построим многочлен над полем $GF(p)$ размерности $n-1$, график которого проходит через подмножество особых точек $D'\subset D$:

$$F(x)=\sum_{i=0}^{n-1} a_i x^i \bmod p, \tag{2}$$

$$F(d'_{xi})=d_{yi} \bmod p. \tag{3}$$

3. На основе построенного полинома выберем произвольные точки и вычислим их координаты, сформировав множество $R=\{r_{xi},r_{yi}\}$ такое, что:

$$\begin{aligned} &|R|=n-t,\\ &r_{xi}\neq d'_{xi}, \end{aligned} \tag{4}$$

где t – произвольное целое число, являющееся константой для алгоритма и определяющее количество точек, необходимых для восстановления полинома ($1<t<n-1$).

Таким образом, $<R,n,p>$ в данной системе является открытой информацией, хранимой в базе данных.

4. Сформируем искомую биометрическую последовательность S путем конкатенации коэффициентов полинома a_i.

Данная последовательность не требует защищенного хранилища, т.к. восстанавливается из вновь полученного отпечатка пальца.

Этапы блока в процедуре регистрации пользователя:

1. Во вновь полученном и предварительно обработанном отпечатке пальца выделим особые точки $D_1=\{d_{1xi},d_{1yi}\}$.

2. Сформируем полином на основе множества R и t точек из D_1, воспользовавшись интерполяционным многочленом Лагранжа:

$$\begin{aligned} &F'(x)=\sum_i l_i(x)y_i,\\ &l_i(x)=\prod_{i\neq j}\frac{x-x_i}{x_i-x_j}. \end{aligned} \tag{5}$$

Все операции в выражении выполняются в конечном поле $GF(p)$.

Восстановить коэффициенты полинома возможно только при условии, что выбранные t точки были использованы при формировании полинома $F(x)$, т.е. мощность множества D_2, являющегося пересечением исходного и вновь полученного множеств особых точек папиллярного узора, не меньше значения t:

$$F'(x)=F(x)\Leftrightarrow |D_2|\geq t, D_2=D\cap D_1. \tag{6}$$

3. Сформируем вновь полученную биометрическую последовательность путем конкатенации коэффициентов полинома $F'(x)$.

Выполнение всех вычислений в пределах конечного поля приводит к высокой точности системы, а использование проблемы восстановления полинома из определенного числа точек – к высокой степени безопасности.

Блок Fuzzy Extractor

Стандартные системы биометрической идентификации обладают серьезным недостатком – биометрический образ или последовательность при каждой генерации соответствуют исходному биометрическому материалу и относительно постоянны. В результате в случае компрометации такой последовательности заменить ее невозможно. Для решения данной проблемы авторами задаются следующие требования к биометрической системе:

– криптографический ключ при каждой процедуре регистрации пользователя в системе должен отличаться от предыдущего;

– один из входных параметров функции генерации ключа должен быть случайным;

– случайный параметр в открытом виде не должен нигде храниться, как и биометрическая последовательность.

Выполнение поставленных требований возможно путем генерации случайной последовательности, используемой в качестве соли в алгоритме генерации криптографического ключа. Алгоритмом решения этой задачи в биокриптографии является Fuzzy Extractor [2], позволяющий выполнить в том числе и требование формирования случайной последовательности (отсутствия хранилища) из вновь сгенерированной биометрической и открытой информации.

Пусть $dis(a,b)$ – расстояние между двумя последовательностями a и b, а l – длина требуемой уникальной последовательности $U \in \{0,1\}^l$, тогда метод генерации уникальной последовательности в контексте схемы fuzzy extractor будет содержать две функции (генерация закрытой последовательности и восстановление данной последовательности, используемой для аутентификации либо дальнейших криптографических преобразований):

1. $Gen(S) = <U,P>$, где S – биометрическая последовательность, полученная в предыдущем блоке; U – сгенерированная случайная последовательность; P – соответствующая открытая последовательность.

2. $\mathrm{Re}p(S',P) = U$, где S' – вновь полученная биометрическая последовательность.

Пусть C – корректирующий код длины k, тогда $C_E : W \to \{0,1\}^k$ – функция кодирования, а $C_D : \{0,1\}^k \to W$ – функция декодирования.

В этом случае алгоритм сводится к следующим выражениям:

1. $P = S \oplus C_E(U)$.

2. $C_D(S' \oplus P) = C_D(S' \oplus S \oplus C_E(U)) = U'$, $U' = U \Leftrightarrow dis(S,S') \le r$, где r – корректирующая способность кода C.

Таким образом, U – битовая последовательность, взаимосвязанная с биометрической информацией и не хранящаяся ни в каком виде, а получаемая каждый раз при генерации биометрической последовательности.

Генерация криптографического ключа на основе битовой последовательности

Выработка криптографического ключа производится на основе битовой биометрической последовательности S.

Для решения данной задачи используется RFC 2898, в частности, стандарт формирования ключа на основе пароля PBKDF2 (Password-Based Key Derivation Function) [3]:

$$K = PBKDF2(S,U,c,dkLen), \tag{7}$$

где S – биометрическая последовательность; U – случайная битовая последовательность, определяющая возможность формирования ключа, отличного от предыдущих на каждом этапе регистрации пользователя в биокриптографической системе; c – количество итераций в PBKDF2; $dkLen$ – длина ключа K.

Алгоритм PBKDF2, в отличие от аналогичных алгоритмов PBKDF и bcrypt, генерирует ключ не фиксированной длины, а заданной в качестве входного параметра, что является преимуществом для биокриптографической системы, поскольку описываемый алгоритм может быть использован для последующего применения в различных криптографических алгоритмах, а не только в тех, которые

используют ключи определенной длины. В декабре 2010 г. PBDKF2 был рекомендован для использования в криптографических системах Национальным институтом стандартов и технологий (National Institute of Standards and Technology, NIST) в США [4].

В результате работы всех блоков рассматриваемого алгоритма формируется открытая информация $<R,n,p,P>$, используемая для восстановления биометрической последовательности S и «соли» U, а также вырабатывается криптографический ключ K.

Создание алгоритмов, основанных на биометрии и криптографии, позволит разработать системы, в которых отсутствуют недостатки обоих направлений, например возможность хищения закрытого криптографического ключа или незащищенность биометрического образа.

Литература

1. Гончаров С.М. Этапы генерации уникальных ключевых последовательностей на основе папиллярного узора отпечатков пальцев / С.М. Гончаров, А.А. Суховей // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – № 1 (21), ч. 1. – С. 97–99.

2. Харин Е.А. Построение систем биометрической аутентификации с использованием генератора ключевых последовательностей на основе нечетких данных / Е.А. Харин, С.М. Гончаров, П.Н. Корнюшин // Матер. 50-й Всерос. межвуз. науч.-техн. конф. – Владивосток: ТОВМИ, 2007. – С. 112–115.

3. Kaliski, B. PKCS #5: Password-Based Cryptography Specification Version 2.0 // RFC 2898. – RSA Laboratories, 2000. – 34 p.

4. Turan M.S. Recommendation for Password-Based Key Derivation / M.S. Turan, E. Barker, W. Burr, L. Chen // NIST Special Publication 800-132. – National Institute of Standards and Technology, 2010. – 14 p.

Гончаров Сергей Михайлович
Канд. техн. наук, доцент, зав. каф. «Безопасность информации и телекоммуникационных систем» Морского государственного университета им. адм. Г.И. Невельского, г. Владивосток,
Тел.: +7-914-707-29-93
Эл. почта: sgprim@smtp.ru, goncharov@msun.ru

Суховей Александр Александрович
Аспирант Морского государственного университета им. адм. Г.И. Невельского
Тел.: +7-902-488-23-10
Эл. почта: sumastal@mail.ru

Goncharov S.M., Sukhovey A.A

The algorithm for generating a cryptographic key based on the singular points of fingerprint

The algorithm for generating a cryptographic key based on the singular points of fingerprint is offered. The algorithm is divided into blocks, which are the main stages of processing. We describe the procedure of forming sequences with a user registration in system and the subsequent stages of the generation of cryptographic keys.
Keywords: fingerprint, cryptography, fuzzy data, key generation, biometric key, papillary lines, unique sequence.
