УДК 681.322.067

Д.О. Косолапов, Е.А. Харин, П.Н. Корнюшин, С.М. Гончаров

Использование рисунка радужной оболочки глаза для генерации ключевой пары

Приводятся сведения о применении биометрических технологий в криптографии, затрудненных нечеткостью биометрических данных. Для получения фиксированных битовых строк заданной длины используется процедура генерации ключевых последовательностей на основе нечетких данных. При помощи известных алгоритмов из полученных строк вырабатывается ключевая пара.

Огромный интерес к биометрии обусловлен рядом объективных причин. В классических парольных системах аутентификации, а также системах аутентификации на основе карт доступа подглядывание или угадывание пароля, кража или изготовление дубликата карты приводят к компрометации всей системы. Более того, законный пользователь, потеряв или испортив карту, теряет возможность доступа к системе. Системы на основе биометрии практически лишены этих недостатков — идентификатор неразрывно связан с самим пользователем, поэтому потеря или изменение идентификатора возможны только в чрезвычайных происшествиях. Кроме того, современные сканеры биометрических данных позволяют обнаруживать попытки использования муляжей [1]. В системах электронной цифровой подписи построение ключевой пары на основе биометрических характеристик пользователя позволило бы значительно усложнить задачу подделки подписи и, следовательно, практически устранить возможность отказа от авторства.

Однако и современные биометрические системы имеют ряд существенных недостатков, связанных с нечеткостью биометрических данных, — система аутентификации должна обеспечивать безопасное хранение самих цифровых образов, а применение биометрии в криптографии затруднено тем, что последняя требует использовать фиксированные битовые строки. Применение хэш-функций к цифровым образам позволило бы решить многие проблемы современных систем биометрической аутентификации и дало бы возможность построения ключевых последовательностей для использования в криптографических приложениях. Чтобы обеспечить возможность применения хэш-функций, необходимо решить проблему выработки уникальных фиксированных битовых строк из нечетких биометрических данных пользователей.

Первые результаты в этом направлении были получены в 2003 г., когда группа ученых из США разработала общие подходы к генерации ключевых последовательностей из нечетких данных (ГКПНД). Суть процедуры, предложенной ими, заключается в использовании помехоустойчивого кодирования с целью устранения незначительных в определенном смысле искажений цифровых образов, получающихся при каждом сканировании биометрических данных человека [2].

При построении ГКПНД одним из главных вопросов является разработка помехоустойчивого кода для метрики, наиболее пригодной к используемой биометрической характеристике [2].

В настоящей работе рассмотрена проблема генерации ключевых последовательностей на основе рисунка радужной оболочки глаза как одной из наиболее надежных и перспективных биометрических характеристик человека. В качестве цифрового образа используется строка длиной 256 байт, получаемая после применения двумерных фильтров Габора к инфракрасному снимку радужной оболочки глаза [3]. Расстояние между двумя образами определяется через метрику Хэмминга.

Было обнаружено, что большинство помехоустойчивых кодов недостаточно эффективны применительно к битовым строкам, полученным из рисунка радужной оболочки. Более того, многократное сканирование и вычисление среднего значения шаблона лишь незначительно снижают средний уровень ошибок.

Принимая все вышесказанное во внимание, предлагается схема пошагового кодирования. На первом шаге групповые ошибки исправляются при помощи кода Рида–Соломона. Затем результат этой обработки поступает на второй шаг, где он обрабатывается кодом Адамара для устранения одиночных ошибок (рис. 1).

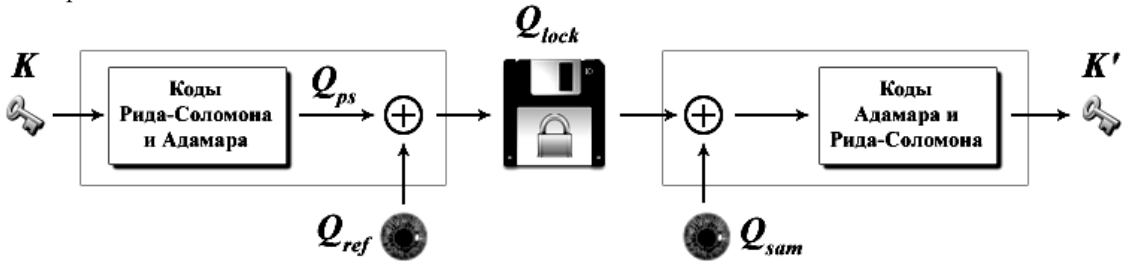

Рис. 1. Схема пошагового кодирования

Ключевая строка K генерируется случайным образом. Затем она последовательно обрабатывается кодами Рида–Соломона и Адамара. В результате этих операций получается псевдоирис-код Q_{ps}, который должен иметь такую же длину, что и реальный ирис-код, — 2048 бит. Далее полученный псевдокод при помощи операции побитового сложения по модулю 2 «блокируется» настоящим ирис-кодом Q_{ref}, предъявленным пользователем.

Для восстановления ключевой строки пользователю необходимо вновь предъявить образец радужной оболочки своего глаза Q_{sam}, после чего все операции повторяются в обратном порядке.

Коды Адамара и Рида–Соломона были выбраны после тщательного исследования различных ошибок, проявляющихся в цифровых образах рисунков радужной оболочки глаза. Изучение множества шаблонов показало, что в большинстве случаев разница между двумя цифровыми образами одной и той же радужной оболочки находится в пределах 10–20% (применение маскирования позволяет снизить этот показатель до 3,37%), в то время как разница между образами разных радужных оболочек находится в диапазоне 40–60% [3].

Для экспериментов была создана база данных, содержащая более 700 образов, полученных от 70 различных пользователей. Образы были получены в лабораторных условиях при помощи одной камеры и на фиксированном расстоянии съемки. 256-байтовые ирис-коды, а также соответствующие им 256-байтовые маски были получены при помощи алгоритма, описанного в [3].

Результаты экспериментов позволяют также определить наиболее оптимальные параметры исправляющих кодов. Так, код Рида–Соломона должен исправлять до 6 ошибок в блоке из 32 бит, а код Адамара — 25% ошибок в каждом блоке. Использование таких параметров позволяет достигнуть уровней ошибок первого и второго рода — 0,5% и 0% соответственно, а также получать ключевые строки длиной 140 бит [3].

Одним из наиболее перспективных направлений в криптографии является криптография на эллиптических кривых (ЭК). ГКПНД позволяют решить задачу получения фиксированной точки на ЭК на основе биометрических данных пользователя.

Пусть K — строка, полученная в результате работы ГКПНД. Для того чтобы получить точку на ЭК $E(F_p)$, можно использовать хэш-функцию

$$H_1: \{0,1\}^* \to G_1,$$

где G_1 — подгруппа точек эллиптической кривой.

Однако вместо того, чтобы непосредственно отображать ключевую строку на подгруппу G_1, рекомендуется сначала воспользоваться стандартной хэш-функцией H, а уже затем полученное значение отображать на G_1, используя детерминированную функцию g, т.е.

$$H_1(U) = g(H(K)).$$

Получив точку эллиптической кривой $P_a = g(H(K))$, можно использовать ее для генерации пары открытый — закрытый ключ:

$$P_s = x * P_a,$$

где x — случайно сгенерированный секретный ключ в F_p^*, а P_s — открытый ключ.

Применение генераторов ключевых последовательностей на основе нечетких данных в биометрических системах позволяет не только повысить их безопасность, но и дает возможность использования биометрических данных в криптографии. Возможность подделки электронной цифровой подписи, равно как и возможность отказа от авторства, в системах, построенных с использованием биометрических технологий, значительно снижены по сравнению с классическими системами ЭЦП, имеющими аналогичные параметры длин ключей.

Литература

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

2. Харин Е.А. Генерация ключевой информации на основе биометрических данных пользователей. //Труды XLV Междунар. Науч. студ. конф. — Новосибирск: НГУ, 2007. — С. 181–187.

3. Hao F., Anderson R., Daugman J. Combining cryptography with biometrics effectively // Technical report #640, http://www.cl.cam.ac.uk/ — Computer Laboratory, University of Cambridge, 2005. — 17 p.

Косолапов Дмитрий Олегович,
Дальневосточный государственный университет, аспирант

Харин Евгений Алексеевич
Дальневосточный государственный университет, аспирант

Сергей Михайлович Гончаров
Дальневосточный государственный университет, к.ф.-м.н., доцент

Павел Николаевич Корнюшин
Дальневосточный государственный университет
Директор ДВРУНЦ по проблемам информационной безопасности, д.ф.-м.н., профессор
Эл. почта: korn@ifit.phys.dvgu.ru.

S.M. Goncharov, P.N. Korniushin, D.O. Kosolapov, E.A. Kharin

Fuzzy biometric data prevents implementation of biometric technologies in cryptography

The procedure of key sequence generation is used for calculation of fixed length bit strings based on fuzzy data. The key pair is generated from these strings with well known cryptosystems.