УДК 004.056.53
DOI 10.21685/2587-7704-2019-4-1-14

Open Access | RESEARCH ARTICLE

Обзор средств создания криптографических ключей из биометрии пользователя

Е. И. Казанцев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. И. Иванов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Переход к цифровой экономике приводит к необходимости создания механизмов повышения доверия к электронным документам, находящимся в открытом информационном пространстве. Ключи, полученные на основе биометрических признаков человека, обладают рядом особенностей, которые создают преимущества при разработке и применении средств криптографической защиты. Применение методов преобразования биометрии человека в его криптографический ключ позволяет не только повысить безопасность биометрических систем, но и дает возможность использования биометрических данных в криптографии. Возможность подделки электронной цифровой подписи и возможность отказа от авторства в системах, построенных с использованием биометрических технологий, значительно снижены по сравнению с классическими системами электронной цифровой подписи.

Ключевые слова: биометрия, криптография, нечеткие экстракторы, нейросетевой преобразователь «биометрия-код».

An overview of products for generating cryptographic keys from user biometrics

E. I. Kazantsev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. I. Ivanov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The transition to a digital economy leads to creation of mechanisms for increasing confidence in electronic documents in the open information space. The keys obtained on the basis of human biometric features have a number of peculiarities that create advantages in the development and use of cryptographic protection products. The use of methods for transforming human biometrics into his cryptographic key allows not only increasing the security of biometric systems, but also makes it possible to use biometric data in cryptography. The possibility of forgery of electronic digital signature and the possibility of repudiation in systems built using biometric technologies are significantly reduced compared to classic electronic digital signature systems.

Keywords: biometrics, cryptography, fuzzy extractors, “biometrics-code” neural network converter.

Биометрия в криптографии

В настоящее время в сфере биометрии и криптографии проводится множество исследований с целью разработки надежного и применимого на практике метода использования биометрических

данных в системах криптографической защиты. Анализ этих исследований выявил, что для обеспечения возможности успешного применения биометрических данных в системах криптографической защиты информации, а именно для генерации криптографических ключей, необходимо учитывать их особенности, а также преимущества и недостатки.

Среди преимуществ биометрических данных при использовании их в качестве источника ключевого материала можно выделить следующие:

– биометрические признаки уникальны;

– биометрические признаки воспроизводимы и всегда готовы к использованию;

– удобство и экономическая эффективность;

– гибкость, сочетаемость разных признаков.

Однако проблемными остаются такие аспекты:

– наличие ошибок первого и второго рода;

– биометрические данные неточно воспроизводимы и не имеют равномерного распределения вероятностей;

– биометрические данные не являются секретными;

– биометрические данные могут меняться со временем и в зависимости от физического и эмоционального состояния их владельца.

Нечеткие экстракторы

Данный способ позволяет однозначно восстанавливать секретный ключ из неточно воспроизводимых биометрических данных. Длина ключа задается в виде параметра, при этом для воспроизведения ключа требуются дополнительные открытые данные, соответствующие ключу, которые хранятся в памяти. Метод нечетких экстракторов извлекает случайную, равномерно распределенную последовательность из первоначальных входных данных и далее правильно восстанавливает ее из любых данных, достаточно схожих с первоначальными. «Нечеткий экстрактор» позволяет получать только один ключ, качество выходной ключевой последовательности которого удовлетворяет всем критериям качества криптографических ключей.

Нейросетевые преобразователи «биометрия-код»

В настоящее время в рамках технического комитета по стандартизации РФ «Защита информации» активно ведутся работы по созданию пакета национальных стандартов, регламентирующих требования к средствам биометрической аутентификации личности, обеспечивающих конфиденциальность, анонимность и обезличенность массового оборота персональных биометрических данных. Одним из наиболее важных стандартов является ГОСТ Р 52633.5–2011 [1], регламентирующий автоматическое обучение нейросетевых преобразователей «биометрия-код». Значимость этого стандарта обусловлена необходимостью регламентации процедуры обучения нейросетевого преобразователя «биометрия-код», построенной на знании кода «Свой» и использовании нескольких примеров биометрического образа «Свой», компрометация которых приводит к тому, что биометрическое средство аутентификации перестает быть высоконадежным и характеризуется только остаточной стойкостью к атакам подбора скомпрометированного биометрического образа.

По требованиям базового национального стандарта ГОСТ Р 52633.0–2006 [2] нейронная сеть преобразователя «биометрия-код» должна обучаться автоматически, при этом после обучения исходные данные (код «Свой» и примеры образа «Свой») должны уничтожаться.

Нейросетевой преобразователь «биометрия-код» – заранее обученная искусственная нейронная сеть с большим числом входов и выходов, преобразующая частично случайный вектор входных биометрических параметров «Свой» в однозначный код криптографического ключа (длинного пароля) и преобразующая любой иной случайный вектор входных данных в случайный выходной код.

Фактически нейросетевой преобразователь «биометрия-код» осуществляет сжатие практически до нуля собственной энтропии биометрического образа «Свой», а для биометрических образов «Чужой» нейросетевой преобразователь «биометрия-код» существенно усиливает энтропию до величины, которая примерно в пять раз меньше ее предельного значения. Необходимо строить специальные автоматы обучения нейронов нейронных сетей преобразователя «биометрия-код». На рис. 1 приведена блок-схема работы автомата обучения одного нейрона.

После обучения каждый нейрон преобразователя «биометрия-код» имеет таблицу связей с биометрическими параметрами и таблицу весовых коэффициентов. Практическая реализация средств криптографической защиты информации упрощается, если вместо полноценного шифрования используется криптографическая хеш-функция [3].

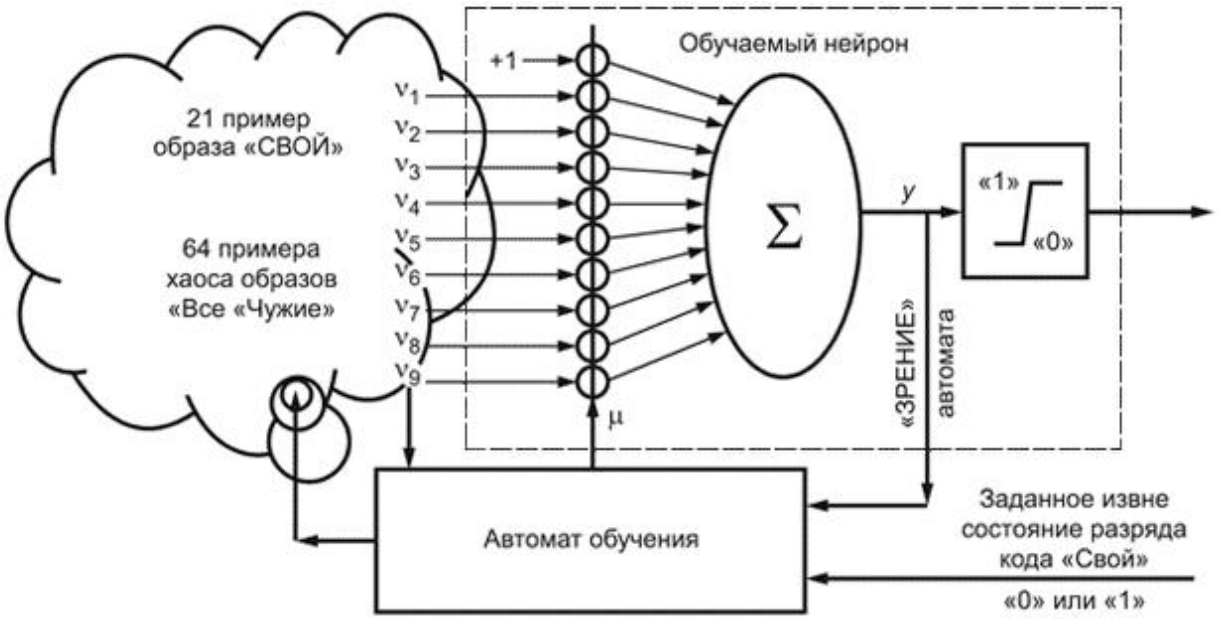

Рис. 1. Блок-схема автоматического обучения одного нейрона нейросети ПБК

Синтез личного криптографического ключа из неоднозначных компонент биометрических данных

Традиционные методы криптографической защиты информации (шифрование, формирование цифровой подписи) обладают низкой эргономичностью. Обычный пользователь не может запомнить длинный пароль из случайных знаков или свой криптографический ключ. В связи с этим активно развиваются методы преобразования личной биометрии человека в его криптографический ключ.

Особенность биометрии заключается в том, что каждый пример реализации одного и того же биометрического параметра будет отличаться от других примеров. Для выделения из них нестабильной компоненты достаточно взять два примера биометрического образа, осуществить центрирование и нормирование их данных и получить разность. Проведя процедуру квантования этой разности, можно получить случайную последовательность.

При вычитании стабильная часть рукописного биометрического образа устраняется, остается его нестабильная часть. Появление нестабильной части биометрических примеров может быть обусловлено множеством факторов, основным из которых является то, что в точности повторить рукописный образ человек не сможет даже в случае попытки обвести его по шаблону.

Для усиления полученной случайной последовательности достаточно получить другую псевдослучайную последовательность от программного генератора и сложить их по модулю два. Также можно усилить случайную последовательность, пропустив ее через нелинейную рекурсивную свертку, например CRC-4 (подсчет контрольных сумм).

Если вычислить криптографическую хеш-функцию от полученной случайной последовательности, то можно использовать ее для получения личного ключа без исследования ее качества.

Библиографический список

1. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия–код доступа. – Введ. с 01.04.2012. – М. : Стандартинформ, 2012.
2. ГОСТ Р 52633.0–2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. – Введ. с 01.04.2007. – М. : Стандартинформ, 2007.
3. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа : моногр. / Б. С. Ахметов, А. И. Иванов, В. А. Фунтиков, А. В. Безяев, Е. А. Малыгина. – Алматы : Издательство LEM, 2014. – 144 с.

Образец цитирования:

Казанцев, Е. И. Обзор средств создания криптографических ключей из биометрии пользователя / Е. И. Казанцев, А. И. Иванов // Инжиниринг и технологии. – 2019. – Vol. 4(1). – С. 1–3. – DOI 10.21685/2587-7704-2019-4-1-14.