Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 9, Пенза-2014, с.79-82 (http://www.pniei.penza.ru/RV-conf/T9/C20)

ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ НА ОСНОВЕ ГОЛОСОВЫХ ОТПЕЧАТКОВ ЧЕЛОВЕКА[1]

Борисов Р.В., Сулавко А.Е., Самотуга А.Е., Еременко А.В. (г. Омск)

В последние годы с повестки дня мировых СМИ не сходят новости об утечках конфиденциальной информации на уровне правительственных и общественных организаций. Анализ ситуации показывает, что злоумышленники в основном используют методы социальной инженерии, а владельцы конфиденциальной информации пренебрегают шифрованием или используют слабые криптографические ключи и пароли. По данным Министерства предпринимательства, инноваций и ремесел Великобритании и Pricewater house Coopers 76% сетевых атак на компании стали возможны из-за ненадежных ключей (паролей). Традиционным способом защиты информации от несанкционированных воздействий является шифрование. Современные алгоритмы шифрования предоставляют достаточно высокий уровень защищенности. Однако вопросы выбора ключей для асимметричного и симметричного шифрования, а также их защиты во время хранения и передачи отнюдь не тривиальны, их проработка требует внушительных финансовых затрат. Если найти устойчивые преобразования для осуществления однозначной и неотъемлемой "привязки" ключа для шифрования к биометрическим характеристикам каждой конкретной личности, данные вопросы можно будет считать закрытыми. Настоящая работа направлена на поиск и разработку таких преобразований для биометрических признаков голоса.

Для того чтобы осуществить генерацию ключа субъект многократно произносит фиксированную парольную фразу [1]. “Привязка” ключа осуществляется не только к субъекту, но и конкретному паролю. Предварительно речевой сигнал при помощи преобразования Фурье трансформируется в амплитудный спектр, затем осуществляется сглаживание полученного спектра в соответствии с формулой (1), далее производится интегрирование сглаженного спектра в окрестности экстремумов по формуле (2) [1, 2].

$$F^*(\nu_j) = \sum_{i=j-n}^{j+n} F(\nu_i)/(2n+1), \quad (1)$$

где $F(\nu_j)$– исходный амплитудный спектр, ν_j– значение частотыj-ого гармонического колебания,n – эмпирически подбираемая величина.

$$F^{**}(\nu_j) = \frac{\sum_{\mu_j=\nu_i-x}^{\nu_i+x} F^*(\mu_j)}{2x+1}, \quad (2)$$

где ν_j–значение частоты, соответствующее экстремуму функции,n – эмпирически подбираемая величина, соответствующее экстремуму функции $F^*(\mu_j)$, x– ширина окна интегрирования.

1 - Работа выполнена в рамках проекта РФФИ № 15-07-09053

Полученные числа являются значениями биометрических признаков. Итоговое количество признаков составило 60 во всех случаях (по аналогии с работой [1]). Таким образом, речевой сигнал преобразуется в массив значений признаков – голосовой отпечаток субъекта, характеризующий как диктора, так и речевое сообщение [1, 2].

Несколько голосовых отпечатков обрабатываются по указанному выше принципу, далее вычисляются средние значения признаков. Полученный массив чисел является эталоном речевого сообщения диктора или эталоном голосового отпечатка.

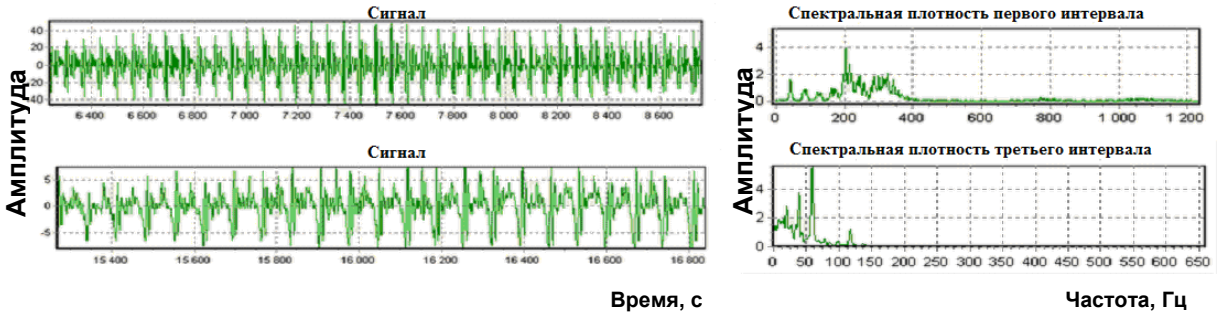

Рис.1.Сигналограммы речевых сообщений и их нормированные амплитудные спектры.

Голосовые отпечатки предлагается использовать для генерации криптографических ключей на основе элементов теории информации. Основной проблемой при генерации ключевых последовательностей по биометрическим данным является техническая невозможность получения одинаковых образов биометрических характеристик при их повторном вводе пользователем. Ситуационные изменения в психофизиологическом состоянии человека, изменения его почерка в течение жизни приводят к проблеме несовпадения биометрических образов одного и того же человека и генерация ключа при этом становится затруднительной. Решить обозначенную проблему возможно с использованием помехоустойчивых кодов, исправляющих ошибки (коды Адамара, Рида-Соломона, Хемминга и др.). Общая концепция построения такого генератора применительно к биометрическим признакам голоса заключается в следующем. Изначально случайным образом генерируется битовая последовательность, которая кодируется помехоустойчивым кодом, далее данная последовательность объединяется с эталонными характеристиками голосового отпечатка (средними значениями признаков). Предварительно (перед объединением) значение каждого признака округляется (в данной работе использовалось округление до сотых) и преобразовывается в целочисленный вид (например, 0,0097342 → 97 → 1100001). Далее осуществляется конкатенация полученных двоичных чисел в строку (назовем ее закрытой строкой). Полученная строка объединяется с закодированной битовой последовательностью. Способ объединения может быть различным –от простого сложения по модулю 2 до использования алгоритмов нечеткого вывода [3]. Результатом объединения является открытая строка. Чтобы получить ключ шифрования субъект снова воспроизводит речевое сообщение, которое обрабатывается соответствующим образом (сначала речевой сигнал преобразуется в голосовой отпечаток, далее производится преобразование голосового отпечатка в

закрытую строку) и «вычитается»из открытой строки (по принципу, обратному способу объединения) для «отсоединения» биометрических данных. После применения кода, исправляющего ошибки к полученной строке, в случае высокой степени «схожести» предъявленного биометрического образа и эталонного (т.е. высокой степени «схожести» полученных из этих образов закрытых строк), будет найдена исходная последовательность битов, которая и является ключом. Это направление реализации процедур выработки криптографических ключей получило название нечетких экстракторов [4] и достаточно подробно описано в доступной литературе.

Пусть существует произвольное пространство цифровых представлений биометрической характеристики *M*, два экземпляра биометрической характеристики длины *l* – *a* и *a'*, т.е. точки пространства *M*, а также *t* – предельное расстояние при котором точки пространства *M*, будут рассматриваться как реализации значений признаков одного субъекта. Пусть также *dis(a,b)* – функция расстояния в пространстве. Тогда точки *a* и *a'* будут принадлежать одному субъекту тогда и только тогда, когда расстояние между ними будет меньше либо равным предельному: $a \approx a' \Leftrightarrow dis(a, a') \leq t$.

Назовем *(M, l, t)* генератором ключевых последовательностей на основе нечетких данных,*(M, l, t)* состоит из двух функций *Gen()* и *Rep()*. *Gen(a)* – генератор, возвращающий две строки: ключевую строку *U* и соответствующую ей «открытую» строку *V*, благодаря которой в дальнейшем возможно получение *U*, используя подходящие биометрические данные. *Rep(a',V)* — процедура, позволяющая восстановить *U* из соответствующей ей «открытой» строки *V* и любой точки *a'* выбранного пространства M, достаточно близкой к *a*. При предоставлении несоответствующих биометрических данных, получение ключевой строки, невозможно:

$$\forall a, a' \in M: dis(a,a') \leq t,$$

$$Gen(a) = (U, V) \Rightarrow Rep(a', V) = U.$$

Пусть *C* – помехоустойчивый код с исправляющей способностью *t*. *Ce: M* → *{0,1}*^{k}– функция кодирования. *Cd: {0,1}*^{k} → *M* – функция декодирования. Тогда генератор в качестве *U* возвращает случайную строку нужной длины, а *V* вычисляет следующим образом: $V = a \oplus Ce(U)$. Тогда *Rep(a',V)*вычисляет:

$$Cd(V \oplus a') = Cd(Ce(U) \oplus a \oplus a') = U',$$

$$U = U' \Leftrightarrow dis(a, a') \leq t .$$

Для получения строки *U* пользователю необходимо предъявить *V* и свои биометрические данные. Компрометация одного из параметров не позволит злоумышленнику восстановить строку *U*.

В настоящей работе предлагается метод генерации ключей на основе голосовых отпечатков с использованием кода Рида-Соломона, аналогично тому, как

это производилось в [5]. В качестве операции объединения и разъединения открытой строки использовалось сложение по модулю 2. В кодах Рида-Соломона контрольные биты распространяют свое влияние на все информационные биты, т.к. данные коды исправляют групповые ошибки, и потому с увеличением количества контрольных бит (исправляющей способности кода), увеличивается и количество распознаваемых/устраняемых ошибок [6]. Важно найти оптимальное количество бит для восстановления. На данный момент по результатам проведенного эксперимента с привлечением 10 испытуемых сумма ошибок 1-ого и 2-ого рода при восстановлении ключевой последовательности в лучшем случае (при оптимальной исправляющей способности кода) составила 0,16 (было проведено всего 100 опытов). Планируется проведение дальнейших масштабных натурных и вычислительных экспериментов с привлечением большего числа испытуемых и большого числа опытов, а также усовершенствование метода генерации ключа посредством реализации операции объединения закрытой строки со случайной битовой последовательностью на основе одного из алгоритмов нечеткого вывода. Также дальнейшие исследования будут направлены на поиск новых информативных признаков.

ЛИТЕРАТУРА:

1. Епифанцев Б.Н., Ложников П.С., Сулавко А.Е., Борисов Р.В. Комплексированная система идентификации личности по динамике подсознательных движений // Безопасность информационных технологий. – 2011. № 4. – С.97-102.

2. Борисов Р.В. Способ формирования голосового отпечатка диктора. Сборник докладов Всероссийской конференции «Научная сессия – ТУСУР 2011», г. Томск, 2011 г. –Т.1. –С. 60-63.

3. Круглов В. В. Нечеткая логика и искусственные нейронные сети : учеб. пособие / В. В. Круглов, М. И. Дли, Л. Ю. Голунов. – М.: Физматлит, 2001. – 224 с.

4. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data // Proceedings from Advances in Cryptology. EuroCrypt. – 2004

5. Еременко А.В., Сулавко А.Е. Исследование алгоритма генерации криптографических ключей из биометрической информации пользователей компьютерных систем // Информационные технологии. «Новые технологии» – 2013. № 11. – С. 47–51.

6. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / пер. с англ. В. Б. Афанасьева. — М.: Техносфера, 2006. — 320 с.

Материал поступил 19.12.2015. Публикуется по положительной рецензии к.т.н. Безяева А.В.