МЕХАНИЗМЫ ГЕНЕРАЦИИ БИОМЕТРИЧЕСКОГО ЦИФРОВОГО КЛЮЧА НА ОСНОВЕ БИОМЕТРИЧЕСКИХ СЕРТИФИКАТОВ

Д.В. Алпеев

Узбекистан, Ташкент, ТУИТ

1 Введение

Сегодня цифровая подпись находит различное применение в области защиты информации: идентификация, обеспечение целостности информации и др. Набирает популярность цифровая подпись полученная на основе биометрических данных пользователя (биологические характеристики в купе с определенными психологическими и физиологическими особенностями индивидуума: отпечатки пальцев, речевые образцы, радужная и сетчатая оболочка глаза, лицо, подчерк и др.). В данной статье предлагается механизм генерации цифровой подписи (пары закрытых и открытых ключей) на основе биометрических данных для создания биометрического цифрового ключа в целях обеспечения достоверной аутентификации и защищенной связи в открытых сетях.

2 Биометрический цифровой ключ и сертификат

Процесс генерации цифровых ключей в биометрической системе представляет собой последовательность выполнения следующих шагов: извлечение характерных биометрических признаков из полученных биометрических данных; сравнение извлеченных биометрических признаков с биометрическими данными хранящимися в базе данных; генерация ключей цифровой подписи на основе биометрических данных (RSA [1],[2] или ElGamal [3]).

Так как биометрические системы аутентификации используют вероятностный метод идентификации пользователя, их уровень достоверности зачастую недостаточно высок. В связи с этим нами предлагается схема повышения надежности биометрической аутентификации на основе использования цифровой подписи и биометрических цифровых ключей. Так, используя пару биометрических цифровых ключей, отправитель (клиент) может безопасно взаимодействовать с получателем (сервером), аутентифицируя друг друга на основе биометрических сертификатов.

Схема генерации биометрического цифрового ключа

В модели генерации ключей (рис. 1) идентичность пользователя удостоверяется путем сравнения полученной биометрической информации с биометрическом сертификатом, хранимым в базе данных биометрического центра регистрации (БЦР) (по аналогии с центром регистрации (ЦР)). Таким образом, только пользователь, зарегистрировавший собственные биометрические образцы в БЦР может создавать свои пары открытых и закрытых ключей. Открытый ключ регистрируется в центре регистрации ЦР.

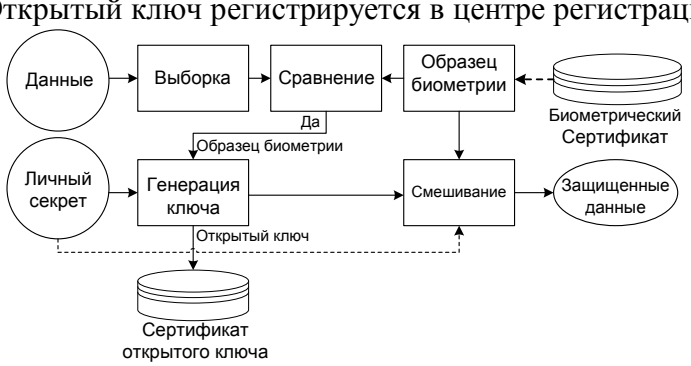

Рис.1 Модель генерации биометрических цифровых ключей

1) Выборка. Данная функция осуществляет выборку биометрического образца из исходных биометрических данных.

2) Генерация биометрического цифрового ключа. Закрытый ключ генерируется хэшированием (MD5 или SHA-1) секретной информации пользователя и биометрического образца.

3) Смешивание. Функцией модуля перемешивания является сокрытие закрытого ключа путем использования биометрического образца и секретной информации (схема «fuzzy vault») [4]: (1) генерация ложного биометрического образца; (2) вычисление полиномов реального и ложного образца и проецирование на них закрытого ключа (3) объединение результатов шага 1 и 2 и получение защищенного образца (биометрический цифровой ключ).

Биометрическая цифровая подпись

На рис.2 изображен механизм генерации цифровой подписи. Сначала производится аутентификация пользователя путем сравнения полученного биометрического образца с биометрическим сертификатом. Если результат сравнения положителен, стартует механизм извлечения закрытого ключа из защищенного образца (биометрического цифрового ключа) с использованием пользовательской секретной информации и биометрического образца. Далее пользователь генерирует цифровую подпись извлеченным закрытым ключом, подписывает документ и пересылает его получателю.

Получателем документа в свою очередь владелец цифровой подписи удостоверяется на основе открытого ключа подписчика документа и биометрического сертификата.

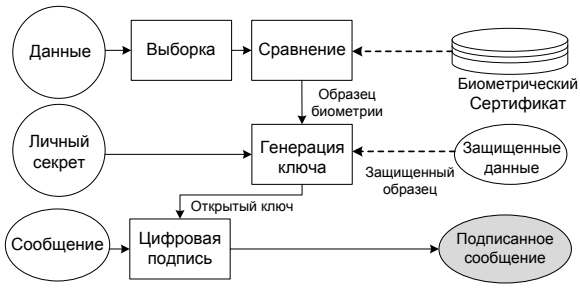

Рис.2 Модель генерации биометрической цифровой подписи

3 Внедрение и результаты оценки производительности схемы

На рис. 3 изображено ПО реализации биометрического шифрования на основе использования в качестве исходных биометрических данных отпечатки пальцев. Первый этап работы разработанного ПО – получение биометрического образца анализируемых отпечатков. Далее производится генерация закрытого ключа на основе биометрического образца и секретной информации и биометрического цифрового ключа. Длина генерированного закрытого ключа в эксперименте 256 бит (однако возможна генерация ключей длиной до 1024 бит).

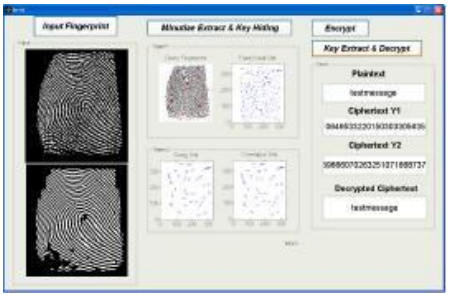

Рис.3 ПО генерации биометрической цифровой подписи

Среднее время генерации цифровой подписи может быть вычислено на основе сложения значений времени работы каждого модуля схемы:

$$T_{общ} = Tbio + Tkey + TFV + Tsig + \varrho \quad (1),$$

где ϱ - пренебрежимо малый коэффициент.

4 Заключение

В данной статье была предложена схема генерации биометрического цифрового ключа. Предложенная модель использует биометрический образец для аутентификации пользователя в процессе генерации, таким образом, только аутентифицированный пользователь может участвовать в данном процессе. Также в данной работе представлено ПО реализации представленной схемы и метод оценки производительности модели.

Литература:

[1] Rivest R., Shamir A., Adleman L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21, 120–126 (1978)

[2] Boneh D.: Twenty years of attacks on the RSA cryptosystem. Notices of the American Mathematical Society (AMS) 46(2), 203–213 (1999)

[3] ElGamal T.: A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. IEEE Transactions on Information Theory 30(4), 469–472 (1985)

[4] Jules A., Sudan M.: A Fuzzy Vault Scheme, Proc. IEEE Int'l Symp. Information Theory, IEEE Press, 408. (2002)