Министерство образования Республики Беларусь
Белорусский государственный университет информатики и радиоэлектроники
Оперативно-аналитический центр при Президенте Республики Беларусь
Государственное предприятие «НИИ ТЗИ»
Центр повышения квалификации руководящих работников и специалистов Департамента охраны МВД Республики Беларусь
Белорусское инженерное общество

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тезисы докладов XVI Белорусско-российской научно–технической конференции (Минск, 5 июня 2018 г.)

Минск БГУИР 2018

УДК 004.56 (043.2)
ББК 32.973.26–018.2

ПЕРЕХОД К НЕДВОИЧНЫМ ПОМЕХОУСТОЙЧИВЫМ КОДАМ В БИОМЕТРИЧЕСКИХ СИСТЕМАХ

Б.А. Ассанович, Ю.Н. Веретило, В. Рудалеску

В последнее время в литературе особый интерес вызывает реализация надежных криптографических систем на основе нечетких экстракторов (Fuzzy extractor), использующих ненадежные «зашумленные» данные биометрических измерений.

Известно, что, если в таких системах возникающий шум, вызванный нечеткостью биометрических данных, является аддитивным и приводит к ошибкам типа замещений, эффективным решением является применение помехоустойчивых кодов с как можно большим расстояния Хэмминга *d*. Один из подходов при создании такой системы является использование конструкции с коррекцией кодом (Code-offset) [1], образующей вспомогательный безопасный эскиз (Secure Sketch), хранящийся в базе данных. Он применяется вместе с корректирующим ошибки (*n, k, d*) кодом и представляет смещение (offset) *D*, «сдвигающее» кодовый вектор *X* применяемого помехоустойчивого кода, содержащего пароль пользователя *S*, на значение биометрического измерения B, т. е. $D = B–X$. При последующем биометрическом измерении B’ выполняется вычитание $D–B’= Y$, декодирование *Y* и получение пароля *S*’, как правило, совпадающего с *S*.

Для достижения необходимой эффективности (минимизации вероятности ошибок пропуска и ложного отказа) используют «мощные» корректирующие коды, например, БЧХ, увеличивая расстояние Хемминга для исправления многократных ошибок [2], а также переходят к недвоичным помехоустойчивым кодам (Рида-Соломона, Турбо-коды) [3], где их эффективность может оцениваться расстоянием Евклида.

В данной работе предлагается реализация нечеткого экстрактора на основе схемы так называемого нечеткого обязательства (Fuzzy commitment) [4] с использованием недвоичных турбо-кодов. Предлагаемая схема обладает лучшими биометрическими характеристиками и гибкостью реализации по сравнению с [2, 3] и обладает возможностью выбора типа недвоичного кода, произвольной длины его блока и величины «предыскажения» для достижения необходимой конфиденциальности и безопасности данных.

Предлагаемая схема включает две основные процедуры: регистрация (Enrollment) и аутентификация (Authentication). Данные пользователя из бинарной формы выбранной длины *d* преобразуются в m-ичные числа, где d степень числа m.

На этапе регистрации m-ичный пароль пользователя (Secret Key) *Sm* поступает в недвоичный кодер (Non-binary Encoder), где добавляются избыточные символы для коррекции ошибок, образуя блоки данных *Xm*, которые проходят через *m*-ичный модулятор (Modulator) и вычитаются из блока биометрических квантованных данных *Bq*, образующегося на выходе квантующего преобразователя (Quantizer). Интервал квантования выбирается с учетом мощности используемого помехоустойчивого кода и заданной защищенности данных пользователя. Результирующий блок данных Dm записывается в базу (Data Base) и храниться вместе с хэшом *h*(*Sm*) в ней. На этапе аутентификации новые данные *B’q* суммируются с *Dm* и образуют вектор *Ym*, поступающий в демодулятор-декодер (Non-binary Decoder). Выходом является пароль *S’m*, хэш-функция которого *h*(*S’m*) сравнивается с *h*(*Sm*).

Применение предложенного метода позволяет значительно улучшить основные показатели эффективности биометрических систем на основе нечетких экстракторов.

Литература

1. Dodis Y., Reyzin L., Smith A. Fuzzy extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. EUROCRYPT, 2004. P. 523–540.

2. Ассанович Б.А., Веретило Ю.Н. Биометрическая база данных на основе HOGструктур и кодов БЧХ // Информационные технологии и системы 2017: материалы междунар. науч. конф. Минск, 25 окт.2017 г. С. 286–287.

3. Maiorana E., Blasi D., Campisi P. Biometric Template Protection Using Turbo Codes and Modulation Constellations. IEEE WIFS, 2012. P. 25–30.

4. Juels A.,