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 HOG-структур 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., Wattenberg M. A Fuzzy Commitment Scheme. ACM CCS, 1999. P. 28–36.

СЛОЖНЫЕ СИГНАЛЫ В СВЧ-ДИАПАЗОНЕ

И.В. Баженова

Проблема формирования сложных сигналов в СВЧ диапазоне является актуальной. С развитием электроники СВЧ и созданием класса различных твердотельных приборов (транзисторов СВЧ, диодов Ганна и ЛПД, сложных диодных и транзисторных структур) открылись широкие перспективы в разработке более эффективных устройств и функциональных узлов – модулей приемо-передающих систем и полностью твердотельных РЛС, а также в многоцелевом освоении СВЧ диапазона. Такие научные направления, связанные с вопросами формирования и обработки сложных сигналов, изучением их спектров, разработкой современных РТС с улучшенными тактико-техническими характеристиками являются актуальными и стимулируют проведение экспериментальных работ [1].

В работе исследованы возможности управления твердотельными источниками СВЧ-энергии, показаны возможности современных технических средств формировать сложные сигналы с практически любым численным значением базы. Обычно при использовании простых (импульсов) сигналов для увеличения дальности действия РЛС необходимо увеличивать энергию сигнала. При ограниченной мощности передатчика это можно сделать только за счет увеличения длительности импульса, что приводит к уменьшению точности

измерения и разрешающей способности по дальности, которые определяются длительностью отклика – его основного пика. При использовании сложных сигналов эта противоречивая взаимосвязь разрешима, т. е. можно увеличивать длительность сложного сигнала, его энергию, сохраняя неизменной ширину спектра. При этом максимальная длительность сигнала будет ограничиваться допустимой мощностью передатчика. Поэтому для повышения точности измерения и разрешающей способности по дальности можно увеличивать ширину спектра.

В рамках поставленной задачи, на основе результатов проведенных экспериментов, выполнены численные расчеты корреляционных свойств полученных сложных сигналов, которые имеют тесную взаимосвязь с двухпараметрической функцией неопределенности.

Литература

1. Лущицкий В.В., Савельев В.Я., Ткаченко Ф.А. Анализ работы и расчет основных характеристик генератора на диодах Ганна с варакторной перестройкой частоты // Радиотехника и электроника. 1984. Вып.13. С. 69–73.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ХРАНЕНИЯ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

О.В. Базылева, Г.А. Пухир

Развитие высоких технологий и тренд мобильности привели к тому, что современное мобильное устройство – смартфон или планшет зачастую используется в качестве мобильного офиса, центра развлечений и инструмента для потребления Интернет-контента. Высокая концентрация деловых и персональных данных приводит к тому, что абстрактная стоимость информации перевешивает цену самого устройства.

В то время как мобильные приложения изначально предлагались как инструменты для повышения производительности и информации, рынок быстро расширялся из-за требований пользователей и наличия инструментов для разработчиков. Ежедневно люди оперируют десятками программ на смартфонах. Многие из них передают конфиденциальную информацию, которая может заинтересовать злоумышленников. Исследователи обнаружили присутствие небезопасных приложений практически в каждой отрасли, включая производственные и финансовые услуги. По оценкам экспертов RiskIQ, более 11 % приложений для банковских операций содержат вредоносное ПО или подозрительный код.

К типовым уязвимостям мобильных приложений по отношению к данным пользователей можно отнести:

1. Небезопасное хранение конфиденциальных данных в незашифрованном виде.
2. Слабые серверные элементы управления на клиентском устройстве.
3. Недостаточную защиту транспортного уровня.
4. Инъекцию на стороне клиента, позволяющую реализовать доступ пользователя к произвольному, ненадежному веб-контенту.
5. Слабую авторизацию и аутентификацию.
6. Неправильную обработку сеансов.
7. Реализацию ненадежных входов, позволяющую приложениям общаться между собой, что может быть использовано злоумышленником для атаки.
8. Утечку данных ввода/вывода, обычно используемые для административных или нефункциональных целях из сторонних каналов.
9. Плохое управление криптоключами с возможностью их восстановления.
10. Раскрытие конфиденциальной информации, учитывая, что скомпилированные исполняемые файлы могут быть подвергнуты реверс-инжинирингу.

Представленная проблема демонстрирует важность срочного решения вопроса безопасности мобильных устройств, как с точки зрения пользователей, так и разработчиков.

Со стороны разработчиков необходимо, чтобы каждое приложение разрабатывалось путем тщательного ознакомления с передовыми методами кодирования, а затем постоянно оценивалось для выявления потенциально возможных недостатков. Одним из наиболее эффективных способов повышения безопасности приложений можно отнести защиту сервисов, к которым подключаются приложения.