справляются самостоятельно – Google и другие поисковики давно умеют искать по картинкам, недавно был запущен Shazam для картин, ИИ неплохо разгадывает даже очень плохие рисунки пользователей. В условиях возрастающей мощи компьютера традиционная графическая капча перестает быть помехой для серьеных злоумышленников и целеустремленных спамеров. Поэтому Google отказался от традиционной интерактивной капчи и вместо этого будет анализировать поведение пользователя самостоятельно. В частности, программа будет фиксировать движения мышки и IP-адрес пользователя. Боты, как правило, передвигают курсор кратчайшим путем, что практически невозможно сделать человеку. Новая капча отображается только в виде окошка, в котором программа сама ставит галочку и сообщает пользователю о том, что он не робот.

Литература

1. Коллинс М. Сетевая безопасность по средствам анализа данных. Чикаго: Университет Чикаго, 2014. 202 с.

2. Столингс, У. Основы сетевой безопасности: приложения и стандарты / У. Столлингс. Изд. 6-е. М.: Массачусетский технологический институт, 2016. 464 с.

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ

В.В. Артемьева, Н.С. Карпович

Квантовое распределение ключей предоставляет возможность: можно передавать секретную информацию по открытому (незащищенному) каналу и при этом быть уверенным в том, что ее никто не перехватил.

Цель – обеспечить безусловную безопасность коммуникаций, основываясь на законах физики. Установлено, что существует множество квантовых криптографических алгоритмов – защищенные квантовые каналы, квантовое шифрование с открытым ключем, квантовое подбрасывание монеты, квантовое вычисление вслепую, квантовые деньги – но большинство из них требуют для своего осуществления полноценного квантового компьютера.

Предложено использование квантовых алгоритмов для формирования и передачи ключевой информации в симметричных криптосистемах. Это позволило получить «сырой» ключ, далее следует усиление секретности, исправление ошибок и согласование ключевой последовательности с помощью специальных алгоритмов. Этот метод позволяет двум сторонам, соединенным по открытому каналу связи, создать общий случайный ключ, который известен только им, и использовать его для шифрования и расшифрования сообщений. Важным и уникальным свойством квантового распределения ключей является возможность обнаружить присутствие третьей стороны, пытающейся получить информацию о ключе.

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 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