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.