

Чтобы отобразить расходы по определенной категории (например, для категории «Развлечения») помесячно для начала необходимо отфильтровать DataFrame по нужному значению нужной колонки, далее с помощью функции resample() переформировать DataFrame помесячно. Далее все, как и в предыдущем примере.

Таким образом, библиотека pandas поддерживает все самые популярные форматы хранения данных, позволяет их анализировать по различным параметрам и визуализировать полученные результаты. Использование данного программного продукта способствует эффективному решению задачи учета личных расходов пользователя.

ЛИТЕРАТУРА

1. Документация pandas [Электронный ресурс]. – Режим доступа: <https://pandas.pydata.org/pandas-docs/stable/index.html> – (Дата обращения: 15.04.2019).

УДК 004.056.55

Студ. К.А. Ермаков

Науч. рук. проф., д.т.н. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ОСОБЕННОСТИ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ КВАНТОВОЙ КРИПТОГРАФИИ НА ОСНОВЕ ПРОТОКОЛА БЕННЕТА

Основной задачей криптографии является зашифрование/расшифрование передаваемых данных. К другим задачам относятся: генерация и распределение ключей, аутентификации сторон и т. п. [1].

Задача согласования ключевой информации, предложенная Диффи и Хеллманом, относится к классическим методам асимметричной криптографии. Согласование ключей может основываться и на технологиях искусственных нейронных сетей [2].

В работе рассматриваются основные идеи относительно нового направления – квантовой криптографии (КК). Задача КК – секретное распределение симметричных (одинаковых) ключей между легитимными пользователями. В отличие от традиционной криптографии, опирающейся на математические методы, квантовая криптография основывается на фундаментальных законах квантовой механики [3, 4]. При попытке «подслушать»/измерить квантовое состояние оно неизбежно меняется, а, значит, если кто-то попытается скопировать ключ во время его распределения, об этом станет известно легитимным пользователям.

Простейший алгоритм генерации секретного ключа – протокол BB84 – первый протокол квантового распределения ключа, который был предложен в 1984 году Ч. Беннетом и Ж. Брассаром [4]. Протокол использует для кодирования информации четыре квантовых состояния двухуровневой системы, формирующие два сопряжённых базиса. Носителями информации являются 2-х уровневые системы, называемые *кубитами* (квантовыми битами), например поляризационные состояния света. Состояния внутри одного базиса ортогональны, но состояния из разных базисов – попарно неортогональны. Эта особенность протокола позволяет отследить попытки «подслушивания» перехватчиком.

Протокол использует четыре квантовых состояния, образующие два базиса, например поляризационные состояния света (рис. 1). Внутри обоих базисов состояния ортогональны, но состояния из разных базисов являются попарно неортогональными, что необходимо для определения возможных попыток нелегитимного съема информации. Таким образом, носителями информации в протоколе BB84 являются фотоны, поляризованные под углами 0° , 45° , 90° , 135° . С помощью некоторого измерения можно различить только два ортогональных состояния [3]:

- фотон поляризован вертикально или горизонтально (базис плюс);
- фотон поляризован под углами 45° или 135° (базис крест).

Отличить горизонтальный фотон от фотона, поляризованного под углом 135° , невозможно.

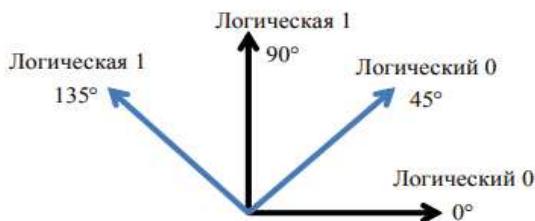


Рисунок 1 – Возможные состояния фотонов

Формирование ключей в протоколе BB84 между сторонами А и В состоит из следующих шагов:

1. А случайным образом выбирает один из базисов (на рис. 1 обозначены в различных оттенках). Затем внутри базиса случайно выбирает одно из состояний, соответствующее 0 или 1, и посылает фотоны (рис. 2). Они могут посыпаться все вместе или один за другим, но главное, чтобы А и В смогли установить взаимно однозначное соответствие между посланным и принятым фотоном.

	/	-	\	-	-	/		
--	---	---	---	---	---	---	--	--

Рисунок 2 – Фотоны с различной поляризацией

2. В случайно и независимо от А выбирает для каждого поступающего фотона (рис. 3): прямолинейный (+) или диагональный (×) базис.

+	+	×	×	+	×	×	×	+
---	---	---	---	---	---	---	---	---

Рисунок 3 – Выбранный тип измерений

Затем В сохраняет результаты измерений (рис. 4).

	-	/	\	-	/	/	/	
--	---	---	---	---	---	---	---	--

Рисунок 4 – Результаты измерений

3. В по открытому общедоступному каналу связи сообщает, какой тип измерений был использован для каждого фотона, то есть какой был выбран базис, но результаты измерений остаются в секрете.

4. А сообщает В по открытому общедоступному каналу связи, какие измерения были выбраны в соответствии с исходным базисом А (рис. 5).

✓		✓	✓	✓		✓
---	--	---	---	---	--	---

Рисунок 5 – Случай правильных замеров

5. Далее пользователи оставляют только те случаи, в которых выбранные базисы совпали. Эти случаи переводят в биты (0 и 1), и получают, таким образом, ключ (рис. 6).

			\	-		/		
1			1	0		0		1

Рисунок 6 – Получение ключевой последовательности по результатам правильных замеров

В таком случае примерно 50% данных выбрасывается. В случае отсутствия подслушивания и шумов в канале связи А и В будут теперь иметь полностью коррелированную строку случайных битов. Если же подслушивание имело место, то А и В должны будут отбросить все свои данные и начать повторное выполнение первичной квантовой передачи. В противном случае они оставляют прежнюю поляризацию. Согласно принципу неопределенности, криptoаналитик (Е) не может измерить как диагональную, так и прямоугольную поляризацию одного и того же фотона. Даже если им будет произведено измерение для

какого-либо фотона и затем этот же фотон будет переслан В, то в итоге количество ошибок намного увеличится, и это станет заметно Алисе. Это приведет к тому, что А и В будут полностью уверены в состоявшемся перехвате фотонов. Если расхождений нет, то биты, использованные для сравнения, отбрасываются, ключ принимается. С вероятностью $1-2^{-k}$ (где k — число сравниваемых битов) канал не прослушивался. Существует оценка, что если ошибка в канале меньше приблизительно 11%, то секретная передача данных возможна.

Квантовая криптография позволяют создавать системы, обеспечивающие практически 100%-ю защиту ключевой информации.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обfuscации : учеб.-метод. пособие для студ. – Минск: БГТУ, 2016. – 220 с.
2. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович // Труды БГТУ. Серия VI. Физико-математические науки и информатика. – Минск: БГТУ. – 2005. – Вып.ХIII.– С.161–164.
3. Лесовик Г. Б. Фундаментальные проблемы физики квантовых технологий. [Электронный ресурс]. – Режим доступа:
<https://mipt.ru/education/chairs/fpfkt/downloads/edumaterials/presentations/presentation.pdf>. – Дата доступа: 15.04.2019.
4. Wikipedia. [Электронный ресурс]. – Режим доступа:
<https://ru.wikipedia.org/wiki/BB8> - Дата доступа: 15.04.2019.

УДК 004.056

Студ. М. Н. Карпович, Е. В. Карпович

Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ШИФРОВАНИЕ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ. УЯЗВИМОСТИ АЛГОРИТМА «РУКОПОЖАТИЯ»

Технология WPA является развитием технологий WEP [1]. Описать эту технологию можно с помощью формальной записи: WPA = 802.1X + EAP + TKIP + MIC, где 802.1X – набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне, EAP – расширяемый протокол аутентификации, TKIP – протокол целостности временного ключа, MIC – проверка целостности сообщений.