$$\chi_*(t) = -2(\alpha+\beta)\ln t + \beta\pi i,$$
$$dW/dt = 8t/\left(\pi\left(1-t^4\right)\right).$$

Для численного решения задачи задаются геометрические параметры α, β ,параметры a, b характеризующие свойства электролита. Численные расчеты формы обрабатываемой границы для этого частного случая проведены при следующих значениях параметров:

$\alpha = 0.25, \beta = 0.25$ .1) – a=-0.301, b=2.401; 2) – a=-0.205, b=1.865; 3) – a=0.21, b=1.28; 4) – a=-0.127, b=1.467; 5) – a=0.141, b=1.104; 6) – a=0.077, b=0.931.

Список литературы

1. Котляр Л.М., Миназетдинов Н.М. Определение формы анода с учетом свойств электролита в задачах электрохимической размерной обработки металлов. //Прикладная механика и техническая физика, 2003, Т. 44, №3, С. 179-184

ЭФФЕКТИВНОСТЬ ПРОТОКОЛА КВАНТОВОЙ КРИПТОГРАФИИ BB84 С КОДИРОВАНИЕМ ОДНОФОТОННЫХ СОСТОЯНИЙ ПО ОТНОСИТЕЛЬНОЙ ФАЗЕ

Румянцев К.Е., Хайров И.Е., Клочко К.В.
Таганрогский государственный радиотехнический университет, Таганрог

В основе наиболее распространенных криптографических систем положен принцип защиты, заключающийся в большой трудности расшифровывания криптограмм и требующих больших вычислительных мощностей. Однако они полностью не исключают возможность расшифровки криптограмм. Одним из наиболее перспективных и достаточно новых направлений в области криптографии является квантовая криптография. В отличие от большинства классических криптосистем, защищенность которых основывается на недоказанных математических предположениях, защищенность квантовых криптографических систем опирается на фундаментальные законы квантовой механики, что при надлежащей реализации таких систем делает принципиально невозможным чтение передаваемых сообщений третьими лицами. Как показывают исследования в данной области, сочетание квантово-криптографических методов распределения секретного ключа и классических методов шифрования позволит создать фундаментально защищенные системы передачи конфиденциальной информации.

Одним из наиболее распространенных в настоящее время протоколов квантовой криптографии является протокол BB84. В данном протоколе однофотонные состояния могут быть промодулированы по поляризации или по относительной фазе. Каждый из этих методов модуляции имеет свои преимущества и недостатки. В частности, поляризационная модуляция наиболее предпочтительна при передаче данных по открытому оптическому каналу, в то время как модуляция по относительной фазе может быть использована в волоконно-оптических системах связи. В случае модуляции фотонов по относительной фазе данный протокол использует 4 фазовых состояния. При этом в зависимости от разности фаз однофотонных импульсов передающего и приемного модулей возможна конструктивная, либо деструктивная интерференции, что определяет передаваемый бит информации.

Проведенные исследования методов съема информации в квантовых каналах с кодированием однофотонных импульсов по относительной фазе позволили выявить наиболее эффективные из них и сформулировать требования к методам защиты. Одним из методов съема является "мощная импульсная атака" [1], при которой нет необходимости напрямую взаимодействовать с квантами света. Следовательно, фазовые системы "Plug&Play" являются уязвимыми по отношению к атакам типа "Троянский конь" [1]. Действительно, Ева может послать сканирующий импульс для выяснения текущего состояния фазового модулятора Алисы (или Боба) и получить его обратно из-за сильного отражения, вызванного зеркалом на конце установки. Для предотвращения подобных видов атак Алиса устанавливает у себя аттенюатор для уменьшения количества света, проходящего через систему. Однако очевидно, что при внесении слишком сильного ослабления система сама окажется неработоспособной. Кроме того, необходимо отслеживать интенсивность принимаемого света при помощи классического детектора, чтобы отследить факт возможной атаки [1].

Так же недостатком системы "Plug&Play" является то, что они не могут работать с настоящими однофотонными источниками и, следовательно, не будут выигрывать от продвижений в области создания таких источников.

Таким образом, проведенные исследования подтвердили актуальность разработки новых методов противодействия атакам в квантовых каналах.

The bibliographic list

1. Vakhitov A.V., Makarov V., Hjelme D.R. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography // Journal of modern optics. 2001.vol. 48. №13. p. 2023-2038.

АНАЛИЗ ЭФФЕКТИВНОСТИ РЕАЛИЗАЦИИ ГОРОДСКОЙПРОГРАММЫ «ЭНЕРГОСБЕРЕЖЕНИЕ»

Тур В.И., Кузин Г.А., Кузина Г.М.
АНО ОС «Ульяновскстройсертификация», Ульяновск

Потенциал энергосбережения в России, по оценке специалистов, составляет 35% от уровня энергопотребления. Около 32% этого потенциала сосредоточено на хозяйствующих субъектах топливно-энергетического комплекса, еще столько же в промышленности, почти 20% в коммунально-бытовом секторе.

Федеральный закон «Об энергосбережении» определяет энергосбережение как реализацию правовых,

организационных, научных, производственных, технических и экономических мер, направленных на эффективное использование энергетических ресурсов, вовлечение в хозяйственный оборот возобновляемых источников энергии, а также снижение средств, расходуемых на оплату энергоресурсов.

В 2002 году в Ульяновске разработана городская программа «Энергосбережение в г. Ульяновске на период до 2006 года».

Реализация государственной энергосберегающей политики в г. Ульяновске должна обеспечить экономическую заинтересованность энергопроизводителей и потребителей в экономии энергетических ресурсов, сократить финансовые затраты потребителей, включая население, на оплату потребляемых ТЭР.

Целью Программы является достижение реальной экономии энергоресурсов и средств, расходуемых на их оплату.

Основные задачи Программы:

- анализ существующего положения в энергосбережении г. Ульяновска;
- разработка нормативно-правовых актов и финансово-экономических механизмов реализации Программы;
- энергоаудит, проведение энергетических обследований организаций и объектов муниципальной сферы;
- энергоучет, оснащение приборами учета жилищного фонда и организаций бюджетной сферы;
- создание системы сопровождения выполненных мероприятий (сервисная служба);
- энергосбережение в системе тепло-, водо- и энергоснабжения г. Ульяновска;
- разработка оптимальной схемы энергосбережения г. Ульяновска;
- энергосбережение в жилищно-коммунальном секторе;
- повышение квалификации кадров;
- энергосбережение в строительном комплексе;
- энергосбережение на транспорте;
- развитие нетрадиционной и малой энергетики;
- информационное обеспечение энергосберегающей политики в г. Ульяновске.

Реализация Программы энергосбережения проводится в два этапа. На первом этапе (2002-2003 г.г.) должны быть разработаны первоочередные нормативно-правовые и методические документы, необходимые для финансово-экономического механизма обеспечения работ по энергосбережению, и начата реализация первоочередных мер по учету и нормированию энергоресурсов, внедрению энергосберегающих мероприятий.

На втором этапе (2003-2006 г.г.) предлагается совершенствование нормативно-правовой, методической и информационной базы в результате всестороннего анализа выполнения работ первого этапа, продолжить разработку и реализацию проектов и мероприятий по различным направлениям энергосбережения, которые позволят снизить расход энергии и бюджетные затраты на дотацию ТЭР.

Анализ реализации Программы показал, что при отсутствии в городе энергосберегающих мероприятий, только в 2003 году, бюджету города и предприятиям ЖКХ пришлось бы изыскивать на оплату теплоэнергии и ГВС дополнительно 126,6 млн. рублей, в том числе 51,1 млн. рублей по социальной сфере.

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРОТОКОЛА КВАНТОВОЙ КРИПТОГРАФИИ BB84 С КОДИРОВАНИЕМ ОДНОФОТОННЫХ СОСТОЯНИЙ ПО ПОЛЯРИЗАЦИИ

Хайров И.Е., Румянцев К.Е.,
Новиков В.В., Троцюк Е.В.
Таганрогский государственный радиотехнический университет, Таганрог

В настоящее время во всем мире уделяется повышенное внимание к системам передачи конфиденциальной информации. Одним из наиболее перспективных и достаточно новых направлений в области криптографии является квантовая криптография. Как показывают исследования в данной области, сочетание квантово-криптографических методов распределения секретного ключа и классических методов шифрования позволит создать фундаментально защищенные системы передачи конфиденциальной информации.

Одним из наиболее распространенных в настоящее время протоколов квантовой криптографии является протокол BB84. В данном протоколе однофотонные состояния могут быть промодулированы по поляризации или по относительной фазе. Каждый из этих методов модуляции имеет свои преимущества и недостатки. В частности, поляризационная модуляция наиболее предпочтительна при передаче данных по открытому оптическому каналу, в то время как модуляция по относительной фазе может быть использована в волоконно-оптических системах связи.

В работе исследуется эффективность протокола квантовой криптографии BB84 с кодированием однофотонных состояний по поляризации. С этой целью разработан пакет программ для ЭВМ, которые позволяют учитывать как параметры передающего и приемного модулей, так и параметры квантового канала связи. При генерации последовательности фотонов на передающем модуле в модели возможны две ситуации:

1) Количество фотонов за длительность оптического импульса строго фиксировано. Данная ситуация позволяет оценить эффективность протокола при использовании идеального однофотонного или многофотонного лазера.

2) Количество фотонов за длительность оптического импульса случайно и подчинено закону Пуассона с заданным средним $\overline{n}$. При этом генерация псевдослучайного числа n, имеющего распределение Пуассона со средним $\overline{n}$, осуществлялась по методу, предложенному Каном. В процессе моделирования проведен анализ этого алгоритма [1]. Сгенерированная таким образом последовательность случайных величин имеет математическое ожидание и дисперсию, отличающиеся от значения $\overline{n}$ на сотые доли