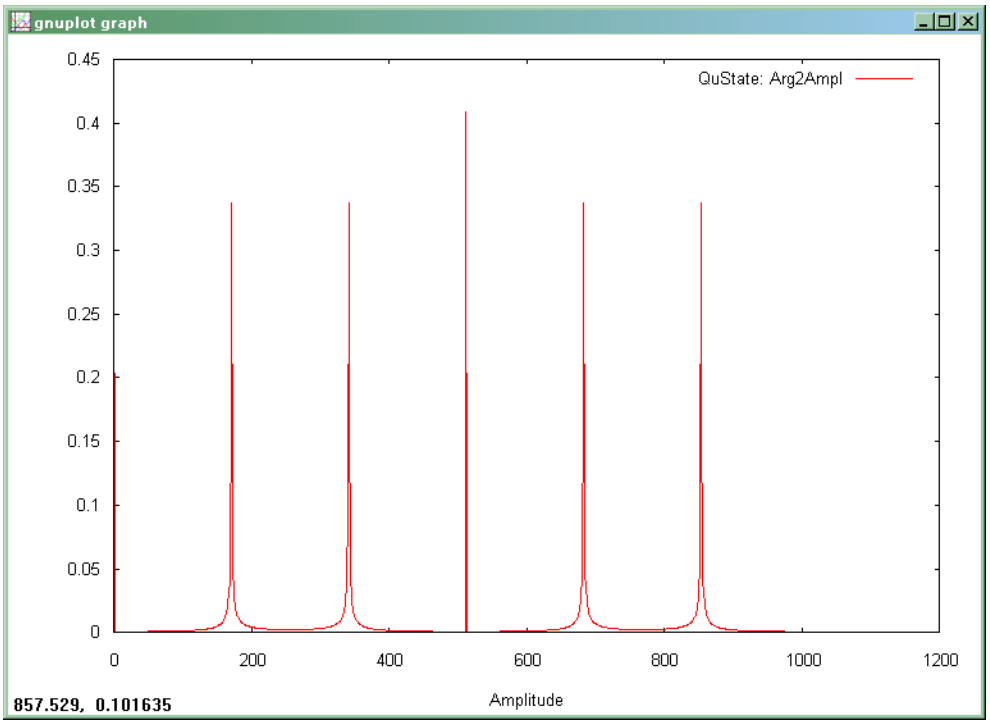

Рисунок 2

V Заключение

Следует отметить, что в настоящее время существует всего лишь несколько алгоритмов в основном для NP-полных задач: алгоритм факторизации целых чисел, алгоритм решения задачи дискретного логарифмирования, и алгоритм поиска элемента в несортированной базе. По-прежнему на данном этапе является открытой проблема возможности создания универсального решения, позволяющего решать широкий круг NP-полных задач с полиномиальной сложностью. Решение данной проблемы может расширить круг возможностей вычислительной техники в областях, связанных как с моделированием квантово-механических физических процессов, эффективным решением задач искусственного интеллекта, так и эффективным решением криптоаналитических задач несимметричной криптографии.

Литература: ***1.*** *Yu. Manin. Computable and uncomputable (in Russian). - Moscow, Sovetskoye Radio, - 1980. – 34-38pp.* ***2.*** *R. Feynman. Simulating physics with computers. - International Journal of Theoretical Physics 21, 6&7, – 1982. - 467-488pp.* ***3.*** *E. Reiffel, W. Polak. Fundamentals of quantum calculations. - ACM Computing Surveys, V. 32, №3, - September 2000. – 5-62pp.* ***4.*** *Брауншгейн С. Л. Квантовые вычисления: учебное руководство. - Encyclopedia of Applied Physics, Update, WILEY-VCH, - 1999, – 35.* ***5.*** *P. W. Shor. Algorithm for quantum computation: Discrete log and factoring. - In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, - November 1994. - 124-134 pp.* ***6.*** *Стин. Квантовые вычисления. - Ижевск: Регулярная и хаотическая динамика, - 2000. – 100 с. 7. B. Omer. Simualtion of Quantum Computers. – Vienna: Technical University of Vienna. - 1996. – 23.*

УДК 621.391.15

МЕТОД ФОРМИРОВАНИЯ СЕКРЕТНОГО КЛЮЧА В КВАНТОВО-КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ КОРРЕКТИРУЮЩЕГО КОДА

Дмитрий Алексеев
Специальный факультет СБ Украины ВИТИ НТУУ «КПИ»

Аннотация: **Предложен метод формирования секретного ключа с использованием корректирующих**

кодов в квантово-криптографических системах (ККС), использующих в качестве носителя единицы информации одно из четырех состояний поляризации единичного фотона.
Summary: **There is proposed method of general key generation with using of corrective code in quantum-cryptography systems (QCS), which use one of the four polarization modes of unit photon as information unit storage.**
Ключевые слова: **Квантово-криптографические системы, квантовая криптография, помехоустойчивые коды.**

I Введение

Основой обеспечения безопасности информации в специальных телекоммуникационных системах (СТС) являются криптографические системы (КС). Известно, что стойкость любой КС определяется секретностью ключа, используемого для шифрования информации. В тоже время, обеспечение безопасной доставки соответствующих ключевых данных законным пользователям является достаточно сложной задачей. Одним из перспективных путей создания доказуемо безопасного канала для передачи ключевого материала является технология квантовой криптографии. В настоящее время разработаны и практически опробованы различные протоколы передачи ключевого материала, анализ которых показывает, что они обладают рядом недостатков: в процессе формирования совместного ключа значительная часть первичного ключевого материала не используется, а его согласование связано с большим объемом многократно передаваемой по открытому каналу информации.

II Постановка задачи

Пусть А и В законные пользователи, использующие для обмена информацией между собой основной (квантовый) канал C_{AB} и канал обратной связи $\overline{C}_{AB}$ (открытый бесшумный канал). Пусть Е незаконный пользователь (противник), знающий весь алгоритм работы метода и обладающий неограниченными вычислительными возможностями (рис. 1).

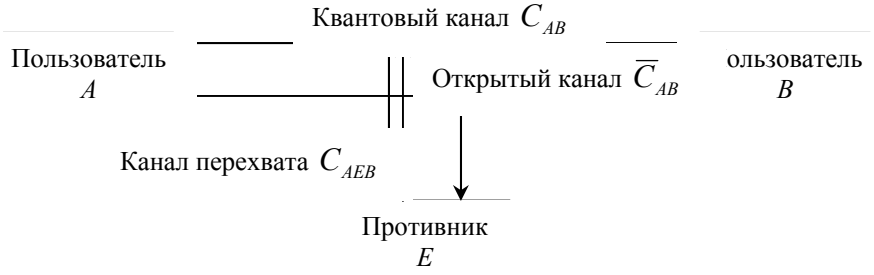

Рисунок 1 – Схема канала связи для передачи ключевого материала

Задачей противника является получение всей или частичной информации о ключе k_{AB}. С этой целью противник может выполнять следующие действия:

1. пассивный противник – читать (но не изменять) все передаваемые по открытому каналу $\overline{C}_{AB}$ сообщения законных пользователей;

2. активный противник – проводит по каналу C_{AE} перехват, детектирование и дальнейшую передачу (канал C_{EB}) пользователю B l фотонов ($0 \le l \le n$), где n – общее количество фотонов, переданных пользователем A.

Каналы C_{AB}, $\overline{C}_{AB}$, C_{AE}, C_{EB} и канал $C_{AEB} \subset C_{AE} \cup C_{EB}$ можно рассматривать как дискретные симметричные каналы с вероятностью ошибки p_{AB}, $\overline{p}_{AB}$, p_{AE}, p_{EB} и p_{AEB} соответственно.

Использование в качестве носителя единицы информации (бита) одного из четырех состояний поляризации единичного фотона имеет принципиальное значение. Согласно законам квантовой физики процедура измерения любого параметра единичного фотона в общем случае неизбежно вносит в его состояние определенное возмущение и результат измерения дает не полную информацию о состоянии системы до измерения [1 – 3]. Проведенные в рамках работы расчеты показали, что при $l = 0$ (отсутствие вмешательства противника) вероятность ошибочного детектирования исходной последовательности a

пользователем B равна $p = p_0 = 0{,}25$, а при $l \to n$, $p_{AB} \neq p_0 \to 0{,}375$ (рис. 2). Видно, что вероятностные характеристики основного канала и канала перехвата взаимно коррелированы: при увеличении достоверности в канале C_{AE} достоверность в канале C_{AB} падает и наоборот.

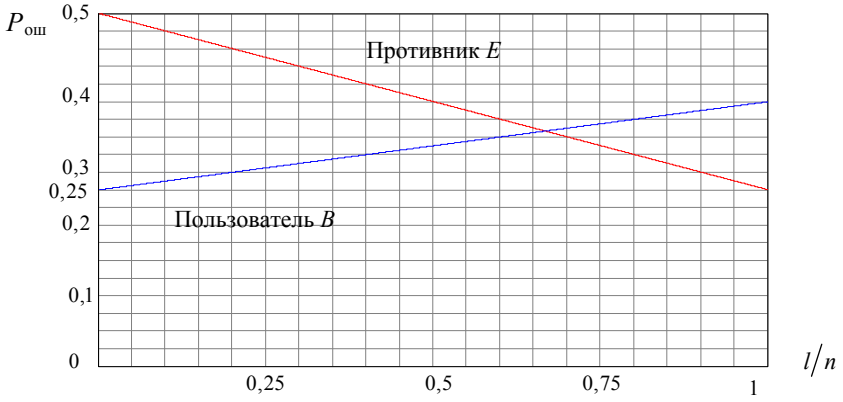

Рисунок 2 – Зависимость вероятности ошибки от относительного количества перехваченных фотонов

Таким образом, задачей данной роботы является разработка метода формирования секретного ключа в квантово-криптографических системах с использованием корректирующего кода, позволяющего, используя физические особенности передачи информации по квантовому каналу и корректирующие свойства помехоустойчивого кода, с высокой надежностью сформировать совместный секретный ключ k_{AB}.

III Формирование ключа при отсутствии вмешательства противника

Рассмотрим общую схему функционирования метода формирования общего секретного ключа с использованием корректирующего кода в квантово-криптографической системе. Условно предложенный метод можно разделить на три этапа.

Первый этап

Целью предварительного этапа является передача по основному каналу первичного ключевого материала – последовательности единичных фотонов. Для этого пользователь A генерирует и передает по основному каналу C_{AB} пользователю B последовательность $a = a_1,...,a_n$ единичных фотонов в одном из четырех состояний поляризации (0^0, 45^0, 90^0, 135^0). Пусть вертикальное (0^0) и диагональное (45^0) состояния означают логическую единицу, а горизонтальное (90^0) и диагональное (135^0) – логический ноль.

Пользователь B фиксирует факт получения фотона и используя два анализатора (прямоугольный и диагональный) проводит побитовое детектирование последовательности $a = a_1,...,a_n$, формируя последовательность $b = b_1,..., b_n$: $b = a \oplus e_k \oplus e_{AB} \oplus e_{AEB}$, где e_{AB} – ошибки, возникающие при детектировании пользователем B; e_{AEB} – ошибки, возникающие из-за перехвата противником; e_k – канальные ошибки (в рассматриваемом методе принимается, что $e_k = 0$); $\oplus$ – покомпонентное суммирование векторов по модулю два.

Выбор направления поляризации на передающей стороне и анализаторов на приемной происходит случайно, равновероятно и независимо друг от друга.

Второй этап

Пользователь B независимо от A генерирует длинную случайную последовательность $s = s_1,...,s_m$, которая:

1. кодируется помехоустойчивым кодом K длины n размерности m $D: s \to x$, для которого известен алгоритм декодирования ψ_A, исправляющий с вероятностью, близкой к 1, ошибки кратности $p_0 n$;

2 для предотвращения утечки информации о ключе к противнику E не более заданной величины

вектор s подается на вход двух различных хэш-функции $\varphi_B(\cdot)$ и $\psi_B(\cdot)$; при хэшировании последовательность s длины m отображается в последовательность z длины t.

Кодовый вектор x покомпонентно складывается с детектированной последовательностью b по модулю два. Полученный вектор $y = x \oplus b = x \oplus a \oplus e_{AB} \oplus e_{AEB}$, а также результат хэш-функции $\varphi_B(s)$ по открытому бесшумному каналу связи $\overline{C}_{AB}$ пользователь *B* передает пользователю *A*.

Третий этап

Получив вектор y, пользователь *A* вычисляет вектор $x' = y \oplus a = x \oplus b \oplus a = x \oplus a \oplus e_{AB} \oplus e_{AEB} \oplus a = x \oplus e_{AB} \oplus e_{AEB}$. С помощью алгоритма декодирования $D^{-1} : x' \to s'$, пользователь *A* вычисляет кодовый вектор $s' = s'_1,\ldots,s'_m$, который с вероятностью, близкой к 1, совпадает с вектором s ($s - s' \to 0$). Необходимым условием правильного декодирования является $H(p_{AB} = p_0) + R < 1$, где $R = 1/6$ – скорость кода [4]. Вектор s' подается на вход хэш-функции $\varphi(\cdot)$, после чего происходит сравнение $\varphi_B(s)$ и $\varphi_A(s')$. При $\varphi_A(s') = \varphi_B(s)$ пользователь *A* проводит количественную оценку вектора ошибок $e = e_{AB} \vee e_{AEB}$, присутствующих в векторе x' на момент подачи его на вход декодера. Для этого пользователь *A* подает вектор s' на вход кодера, аналогичного кодеру пользователя *B* $D : s' \to v$. Результирующий вектор ошибок $e = v \oplus a \oplus y = v \oplus a \oplus a \oplus x \oplus e_{AB} \oplus e_{AEB}$. Если $\varphi_A(s') = \varphi_B(s)$, то $v = x$ и $e = e_{AB} \oplus e_{AEB}$, после чего выполняется сравнение e и $e = p_0 n$.

Общий секретный ключ (при $\varphi_A(s') = \varphi_B(s)$) вычисляется посредством подачи вектора s' на вход хэш-функции $\psi(\cdot)$, отличной от $\varphi_A(s')$.

IV Формирование ключа при наличии вмешательства противника

Противник на первом этапе имеет возможность перехвата, детектирования и дальнейшей передачи законному пользователю *B* l ($0 < l < n$) фотонов. Результатом детектирования противником является последовательность $c = c_1,\ldots,c_l$: $c = a \oplus e_{AE}$, где e_{AE} – ошибки, возникающие при детектировании. Из открытого канала $\overline{C}_{AB}$ противник получает вектор y и значение $\varphi_B(s)$. В работе [5] показано, что оптимальной процедурой обработки последовательности c и y для *E* является их покомпонентное суммирование по модулю два. Полученный вектор $r = c \oplus y = a \oplus e_{AE} \oplus x \oplus a \oplus e_{AB} \oplus e_{AEB} = x \oplus e_{AE} \oplus e_{AB} \oplus e_{AEB}$ является искаженным кодовым вектором кода K. Как и для пользователя *A* условием правильного декодирования вектора r является $H(p_{AE}) + R < 1$. При $H(p_{AE}) + R > 1$ противник с вероятностью, близкой к 1, не сможет правильно декодировать вектор r. Альтернативой для *E* является декодирование r в список объема *N*, в который с вероятностью μ входит кодовый вектор s. Объем списка N оценивается снизу через вероятности p_{AE} и μ следующим образом [6]:

$N \geq 2^{nH(p_{AE})+k-n+\log_2 \mu}$.

Дальнейшее определение секретного ключа может выполняться вычислением $\varphi(\eta)$, $\eta \in N$ с последующим сравнением с значением $\varphi_B(s)$.

V Требования к хэш-функциям

Проведенный в ходе исследования анализ особенностей применения хэш-функций позволяет сформулировать требования, предъявляемые к ним [7].

1 *Сжатие* – функция h отображает входное сообщение x произвольной конечной длины, называемое прообразом, в хэш-значение $y = h(x)$ небольшой фиксированной длины.

2 *Простота вычисления* – для заданной функции h и сообщения x, $h(x)$ вычисляется не выше, чем с полиномиальной сложностью.

3 *Стойкость к вычислению прообраза* – невозможность нахождения неизвестного прообраза для любых предварительно заданных хэш-значений, т. е. для заданной хэш-функции h вычислительно невозможно найти неизвестный прообраз x при предварительно заданном хэш-значении $y = h(x)$ для любого значения y. Под термином "вычислительно невозможно" здесь и далее будем понимать, что алгоритм, выполняющий данное преобразование, обладает не менее чем экспоненциальной сложностью.

4 *Стойкость к вычислению второго прообраза* – невозможность нахождения любого другого прообраза, который давал бы такое же хэш-значение, как и заданный, т. е. для заданной хэш-функции h и прообраза x вычислительно невозможно найти другой прообраз $x' \neq x$, для которого выполнялось бы условие $h(x) = h(x')$.

5 *Стойкость к коллизиям* – невозможность нахождения двух прообразов, для которых вырабатывалось бы одинаковое значение, т. е. для заданной хэш-функции h вычислительно невозможно найти два прообраза x и x', $x \neq x'$, для которых выполнялось бы условие $h(x) = h(x')$.

6 *Отсутствие корреляции* – входные и выходные биты не должны коррелировать, т. е. изменение любого входного бита приводит к большим непредсказуемым изменениям выходных бит.

7 *Стойкость к близким коллизиям* – для заданной однонаправленной функции h вычислительно невозможно найти два прообраза x и x', для которых хэш-значения $h(x)$ и $h(x')$ отличались бы на малое количество бит.

8 *Стойкость к частичной однонаправленности* – вычислительно невозможно восстановить любую часть входного сообщения так же, как и все сообщение. Более того, по любой известной части входного сообщения вычислительно невозможно восстановить оставшуюся часть (восстановление t неизвестных бит требует не менее чем 2^{t-1} операций).

VI Применение корректирующего кода

Следует отметить, что правильный выбор корректирующего кода, а также его параметров является важным этапом разработки предложенного метода. Требования к корректирующему коду определяются характеристиками (свойствами) канала связи, поэтому параметры кода выбираются исходя из вероятности ошибки в основном канале $p_{\text{АВ}} = p_0 = 0{,}25$ Требованием к корректирующей способности кода является выполнение условия: незначительное увеличение $p_{\text{АВ}}$ должно с вероятностью, близкой к 1, приводить к ошибочному декодированию кодового вектора x'.

В качестве корректирующего кода предлагается применять турбокод, образующийся при параллельном каскадировании нескольких компонентных сверхточных кодов, разделенных перемежителем. Возможность применения турбокодов в ККС обусловлено рядом факторов [8, 9]:

1 возможностью формирования длинного блока;

2 применением алгоритмов вероятностного декодирования с использованием априорных вероятностей декодируемых символов на входе декодера и формированием решений о каждом декодированном символе с оценкой степени надежности этого решения (декодирование с гибким выходом);

3 каскадной структурой кода, позволяющей существенно упростить процедуры кодирования и декодирования;

4 итеративным декодированием (многократным использованием одного декодера); это конструктивный путь построения декодера длинных кодов;

5 возможностью выбора оптимальных параметров кода благодаря большому количеству возможных вариантов построения кода (тип перемежителя, выбор составных кодов, регулируемая скорость, алгоритм декодирования)

VII Заключение

Предложенный метод формирования секретного ключа в ККС с использованием корректирующего кода имеет ряд отличий от предложенных ранее: при требуемом уровне безопасности значительно увеличен объем используемого первичного ключевого материала и сокращено количество раундов обмена информацией по открытому каналу. Дальнейшие исследования следует проводить в направлении разработки методики выбора оптимальных параметров кода для реализации предложенного метода.

Результаты работы целесообразно использовать при разработке перспективных ККС в специальных информационно-телекоммуникационных системах.

Литература: 1. Bennett C. H., Bessette F., Brassard G., Savalle L. and SmolinJ., Experimental Quantum Cryptography, Proceedings of Eurocrypt '90, also in Journal of Cryptology, Vol. 5, No. 1 (1992).-P. 3-28. 2. Huges R. G., Buttler W. T., Kwiat P. G., Luiher G. G., Morgan G. I., Nordholt J. E., Peterson C. G., Simmsons C. M. Secure communications using quantum cryptography. – Los Alamos National Laboratory. LA-UR-97-1099.3. Townsend P., 1997b, Quantum cryptography on multiuser optical fiber networks, Nature (London) 385.-P. 47–49. 4. Shannon C. A mathematical theory of communication // Bell Syst.Tech. J. – 1948. – Vol. 27. – P. 379–423. 5. Maurer U. "Secret Key Agreement by Public Discussion Based on Common Information" // IEEE Trans. on IT., Vol. 39, May 1993, pp. 733 – 742. 6. Седельников В. М. Алгоритм выработки общего ключа с использованием квантового канала // Проблемы передачи информации Т.35, №1, 1999.–С.100-109. 7. В. Н. Вервейко, А. И. Пушкарев, Т. В. Цепурит. Функции хэширования: классификация, характеристика и сравнительный анализ//Радиотехника: Всеукр.межвед.науч.-техн.. сб. 2002. Вып. 126 С172-179. 8. Berrou C., Glavieux A. Near optimum error correcting coding and decoding: turbo-codes // IEEE Trans. on Commun. – 1996. – Vol.44, №10. – P. 1261-1271. 9. Банкет В. Л., Прокопов С. Д. Эффективность применения турбо-кодов в телекоммуникационных системах // Наукові праці УДАЗ ім. О. С. Попова. – 2000. – №3. – с. 36-41.

УДК 681.3

ПРИМЕНЕНИЕ ТУРБОКОДОВ В СПЕЦИАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Сергей Зайцев, Сергей Ливенцев, Дмитрий Алексеев
Специальный факультет СБ Украины ВИТИ НТУУ «КПИ»

Аннотация: **Рассмотрены вопросы применения турбокодов в специальных телекоммуникационных системах. Указаны основные принципы построения турбокодов и их характеристики.**
Summery: **There are considered problems of turbocode using in special telecommunication systems in the article. There are showed basic principles of turbocode building and they characteristics.**
Ключевые слова: **Помехоустойчивое кодирование, турбокоды, итеративное декодирование.**

I Введение

Одним из перспективных направлений совершенствования характеристик специальных телекоммуникационных систем является применение корректирующих кодов. В настоящее время широкое распространение в телекоммуникационных системах получил класс помехоустойчивых кодов – турбокоды. Однако в существующей литературе описанию характеристик и способов построения составных кодов уделено не достаточно внимания. ***Целью работы*** является рассмотрение структуры построения турбокодов и их основных характеристик.

Турбокоды используются в качестве метода канального кодирования [1, 2] в системах передачи телеметрической информации с космических аппаратов по рекомендации *CCSDS (Consultative Committee for Space Data Systems),* системах подвижной радиосвязи третьего поколения *UMTS* (*Universal Mobile Telecommunications System*) и *cdma*2000, системах цифрового телевизионного вещания стандарта *DVB-RCS* (*Digital Video Broadcasting Return Channel for Satellite*), спутниковых модемах с повышенной энергетической эффективностью *SDM*-300a, *CDM*-550.

II Постановка задачи

Задачей, решаемой в работе, является описание характеристик составных элементов турбокодов. Для решения поставленной задачи рассмотрим основы теории построения компонентных кодов. Турбокод образуется при параллельном каскадировании двух или более свёрточных кодов, называемых компонентными, разделённых перемежителем. В связи с этим турбокоды иногда называют параллельными каскадными свёрточными кодами. Если в роли компонентных кодов используются стандартные блоковые коды – коды Хэмминга, БЧХ либо Рида-Соломона – то такие коды называют параллельными каскадными блоковыми кодами [2, 3, 4].

В турбокодах используются следующие положения теории кодирования [1 – 3]:

1 длинные коды с шумоподобной структурой обеспечивают предельно достижимую пропускную