УДК 004.056.55 DOI: 10.18698/2541-8009-2018-05-319

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА ПРОТОКОЛА BB84

Е.М. Чередanова pankooova@mail.ru
SPIN-код: 1619-5499

Е.А. Мамченко liza.98.98@mail.ru
SPIN-код: 2887-3715

А.М. Марчук marchuk.sasha2010@yandex.ru
SPIN-код: 9253-5492

А.А. Речкунов recha.art@mail.ru
SPIN-код: 5018-1702

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Задача данного исследования заключается в математическом моделировании в среде MATLAB квантового распределения ключа протокола BB84 и оценке криптографической стойкости передаваемой информации к атакам полного перебора значений (типа brute force). Передача сообщения по квантовому каналу связи осуществляется посредством генерации случайных битовых векторов, которые демонстрируют выбор базисов поляризации и измерения и процесс согласования ключа по классическому каналу связи. Полученное в ходе математического моделирования количество возможных значений, подлежащих полному перебору, чрезвычайно велико, время перебора таких значений оказалось существенно больше срока актуальности и ценности перехватываемой информации. Целью данной работы является исследование криптографической стойкости квантового распределения ключа протокола BB84 и его устойчивости к атакам типа brute force.

Ключевые слова

Криптография, квантовая криптография, шифрование, протокол BB84, квантовое распределение ключа, криптографическая стойкость, квантовое распределение ключа, неопределенности Гейзенберга

Поступила в редакцию 11.05.2018

Теория квантового распределения ключа. Изучение алгоритмов и протоколов метода квантового распределения ключа (КРК) представляет собой перспективное направление развития принципиально новых систем и средств защиты информации. Используя КРК, можно организовать передачу ключа, конфиденциальность которого основана не на ограниченных вычислительных или технических ресурсах злоумышленника, а на фундаментальных квантово-механических законах. Таким образом, квантовая криптография представляет собой метод защиты коммуникаций и средств связи, основанный на использовании принципов квантовой физики. Процесс передачи и приема информации всегда выполняется физическими средствами и с использованием физических принципов, например, с помощью электронов в электрическом токе или фотонов

в линиях волоконно-оптической связи, а перехват и прослушивание могут рассматриваться как измерение определенных параметров физических объектов, в нашем случае — переносчиков информации [1, с. 37].

В основе метода КРК лежит принципиальная неопределенность поведения квантовой системы. Во-первых, используется тот факт, что если наблюдаемые величины описываются некоммутирующими операторами, то их одновременное измерение принципиально невозможно в силу соотношения неопределенностей Гейзенберга. Во-вторых, метод опирается на существующую теорему о запрете клонирования — невозможности копирования заранее неизвестного квантового состояния [2, с. 25].

Используя явления, типичные для квантовых объектов, можно спроектировать и создать такую систему связи, которая всегда может обнаруживать прослушивание: попытка измерения взаимосвязанных параметров в квантовой системе вносит в нее нарушения, разрушая исходные сигналы. Это означает, что по уровню шума в канале легитимные пользователи (Саша и Ваня) могут распознать степень активности перехватчика (Леша). Возможности передачи сообщений по квантовым каналам связи сегодня активно исследуются. Одним из наиболее изученных протоколов (как в теоретическом, так и в практическом аспекте) является протокол BB84, разработанный в 1984 г. Ч. Беннетом и Ж. Брассардом.

В протоколе КРК BB84 используется квантовый канал связи (рис. 1), под которым понимают совокупность передатчика (лазер), приемника (фотодетектор) и среды распространения (оптоволоконный кабель). Передача сообщения осуществляется с помощью двухуровневой квантовой системы — кубита.

Рис. 1. Схема передачи информации по квантовому каналу связи

Состояние кубита описывается вектором в некотором сепарабельном гильбертовом пространстве, порожденным стандартным скалярным произведением, наделенным стандартной нормой, где кет-вектор Дирака допускает два собственных классических состояния — нуль и единица — с соответствующими вероятностями обнаружения $|\alpha|^2$ и $|\beta|^2$:

$$|\psi\rangle = \alpha|1\rangle + \beta|0\rangle, \qquad \alpha, \beta \in C: \ |\alpha|^2 + |\beta|^2 = 1. \tag{1}$$

В случае протокола BB84 переносчиком информации является фотон (квант электромагнитного поля), поляризованный в одном из двух ортогональных базисов:

$$|45\rangle = \frac{1}{\sqrt{2}}(|90\rangle + |0\rangle), \qquad |135\rangle = \frac{1}{\sqrt{2}}(|90\rangle - |0\rangle). \tag{2}$$

Выбор базиса поляризации (1) и (2) является случайным. Углы поляризации в каждом базисе соответствуют классическим битам информации: нулю и единице. После поляризации фотон передается в канал (оптоволоконный ка-

нал) и измеряется на приемном конце, причем базис направления поляризатора при измерении также выбирается случайным образом. Если базис поляризации фотона и базис, в котором он измерен, не совпадают, измерение считается недостоверным [4, с. 175].

В связи с этим наряду с непосредственным распространением ключа по квантовому каналу связи необходим алгоритм согласования, который осуществляется по классическому каналу связи, доступному для прослушивания. Можно выделить следующие типы атак на квантовый канал связи:

– brute force (полный перебор): метод полного перебора всех возможных комбинаций ключа;

– man in the middle (атака посредника): внедрение устройств, осуществляющих перехват информации в середине тракта приема-передачи информации.

Возможные сценарии атак второго типа в настоящее время достаточно хорошо изучены. Для протокола КРК BB84 найдены некоторые эффективные атаки, например, атака за счет разбиения числа фотонов (Photon Number Splitting — PNS-атака, или), основанная на пуассоновской статистике лазерного излучения на передающей стороне. Отметим, что активно изучаются и методы противодействия, которые базируются на исследовании возможности создания истинно однофотонных источников [5, с. 3122].

В связи с развитием средств и методов атак типа brute force (например, с использованием параллельных вычислений, радужных таблиц и метода ветвей и границ) важной является оценка криптографической стойкости КРК к атакам такого типа с учетом особенностей реализации протокола КРК BB84 и процедуры согласования ключа.

Самым важным достижением в области квантовой криптографии можно считать то, что была доказана возможность существенного повышения скоростей передачи — до 1 Мбит/с и более. Увеличение скорости достигается путем уплотнения данных по длинам волн в волоконно-оптической системе. Разделение каналов по длинам волн позволяет реализовать как последовательную, так и одновременную работу открытого высокоскоростного и секретного квантового каналов связи. Одновременно с этим можно говорить и о повышении скорости передачи информации по квантово-оптической криптографической системе при использовании разделения каналов. Это может быть достигнуто благодаря одновременной организации нескольких квантовых каналов по одной общей среде передачи — одному оптическому волокну. В настоящее время в одном стандартном оптическом волокне можно организовать около 50 каналов.

С учетом известных экспериментальных результатов по созданию квантово-оптических криптографических систем в ближайшие годы можно прогнозировать достижение следующих значений параметров [6, с. 18]:

– скорость при относительном количестве ошибок, не превышающем 4 %, — 50 Мбит/с;

– максимальная длина квантового оптического канала связи — 50 км;

– количество подканалов при разделении по длинам волн — 8–16.

Математическое моделирование передачи сообщения по квантовому каналу связи в среде MATLAB. В среде MATLAB моделируется передача сообщения по квантовому каналу связи посредством генерации случайных битовых векторов, которые демонстрируют выбор базисов поляризации и измерения и процесс согласования ключа по классическому каналу связи. С использованием процедуры побитового сравнения можно найти значение совпавших битов в двух случайных битовых векторах, т. е. размер ключа после согласования. По этому значению можно оценить криптографическую стойкость — определить количество комбинаций, которые подлежат полному перебору в атаках типа brute force [7, с. 1131].

Длина ключа $S(N)$ ограничена сверху в асимптотическом смысле размером первоначального сообщения N (т. е. размером битового вектора):

$$S(N) \in O(N) \;\; \exists\, (0 < C < 1) : \; S(N) \leq CN. \qquad (3)$$

В связи с этим более строго определить задачу можно в численной оценке значений параметра C из выражения (3).

Общая структура рассматриваемого квантово-криптографического алгоритма представлена на рис. 2.

Рис. 2. Алгоритм передачи информации по квантовому каналу связи

Как было отмечено ранее, задача построения случайных последовательностей нулей и единиц (случайных значений битового вектора) широко исследуется с математической точки зрения [8, с. 641].

Статистические свойства, присущие только случайным битовым последовательностям, обобщены в статистических тестах Национального института стандартов и технологий NIST (The National Institute of Standards and Technology). Для решения поставленной задачи рассматривали последовательности, состоящие из N символов, где N достаточно велико [9, с. 676].

Для того чтобы построить случайную последовательность, которую можно получить только неалгоритмически, использовали электронный генератор белого шума.

В качестве необходимого условия проверки полученной последовательности проводили частотный побитовый тест, который состоит в определении соотношения между нулями и единицами в битовом векторе. Задача исследования состояла в определении того, насколько соотношение числа нулей N_0 и числа

единиц N_1 близко к 0,5. Для каждого из сгенерированных битовых векторов результаты представлены в таблице, где $R(P_i)$ — отношение числа нулей к числу единиц в битовом векторе P_i [10, с. 55].

Результаты частотного побитового теста

№ п/п	N	N_1 в P_1	N_0 в P_1	N_1 в P_2	N_0 в P_2	$R(P_1)$	$R(P_2)$
1	3 000	1 496	1 504	1 508	1 492	0,4986	0,5026
2	4 000	1 979	2 021	1 972	2 028	0,4947	0,4930
3	9 000	4 442	4 558	4 524	4 476	0,4935	0,5026
4	12 000	6 091	5 909	5 935	6 065	0,5076	0,4945
5	16 000	7 995	8 005	8 050	7 950	0,4997	0,5003
6	20 000	9 938	10 062	9 958	10 042	0,4969	0,4979

Далее было проведено спектральное исследование, основанное на оценке высоте пиков дискретного преобразования Фурье. Для моделирования в MATLAB использовали функцию FFT битового вектора. Необходимо, чтобы число пиков, превышающих пороговое значение в 0,95 по амплитуде, было значительно больше 0,05 [11, с. 82]. Результаты спектрального теста для каждого из используемых в моделировании битовых векторов представлены на рис. 3.

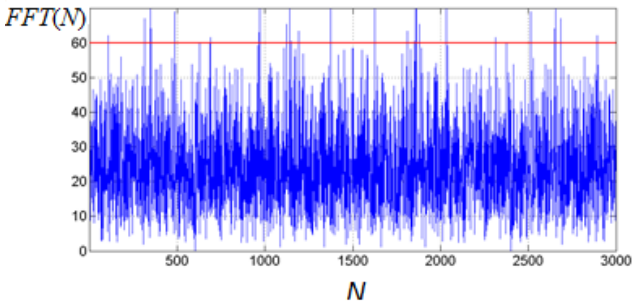


Рис. 3. Результат спектрального теста NIST

Результаты частного и спектрального тестов подтвердили случайность выбранных последовательностей. Таким образом, исходными данными для моделирования являются два случайных битовых вектора P_1 и P_2.

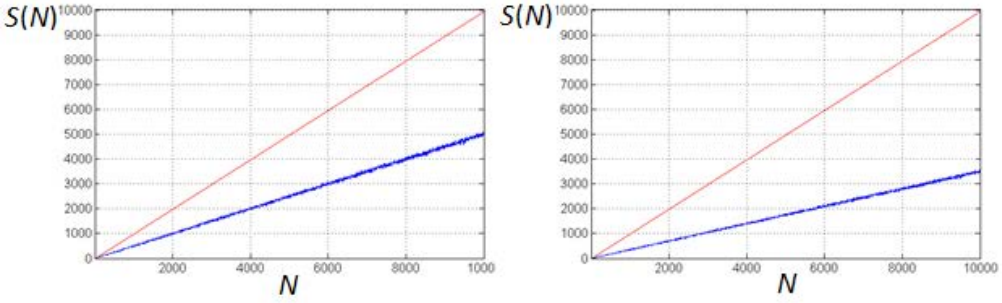
Для оценки длины ключа проводили побитовое сравнение между случайными битовыми векторами. Результаты в форме зависимости значения ключа от размера передаваемого сообщения представлены на рис. 4, *а*.

Типичные значения C в выражении (3) составляют 0,46…0,54 в случае канала без шума. Во-первых, это означает, что вектор, описывающий состояние фотона, подвергается в канале унитарному преобразованию. Во-вторых, это означает, что ошибки при синхронизации ключа отсутствуют.

Шумы в квантовом канале уже достаточно широко изучены. В то же время ошибки, связанные с синхронизацией ключа при обмене сообщениями по клас-

сическому каналу связи, также возможны и могут быть вызваны различными причинами, например, несанкционированным доступом. В идеальном случае классический канал выполняет с передающимся при синхронизации битовым вектором матричное преобразование, причем матрица является единичной. В случае мультипликативного шума исходная матрица умножается (в достаточно общем случае) на матрицу, у которой вне главной диагонали присутствуют единицы. [12, с. 204–205]. В таком случае можно ввести меру шума η, которая характеризуется отношением количества единиц к числу нулей вне главной диагонали матрицы. При наличии такой активной атаки в классическом канале связи необходимо проводить повторную процедуру согласования по более защищенному каналу. Очевидно, что типичные значения в таком случае значительно меньше.

Результаты теста в случае, когда такая активная атака все имела место при соотношении η = 0,3, представлены на рис. 4, *б*. Значение константы (3) составляет 0,22…0,30.



а *б*

Рис. 4. Зависимость значения ключа от размера передаваемого сообщения (с асимптотой)

Общее число комбинаций для атаки типа brute force равно 2^{CN}. При достаточно больших значениях N это значение растет, очевидно, очень быстро (рис. 5).

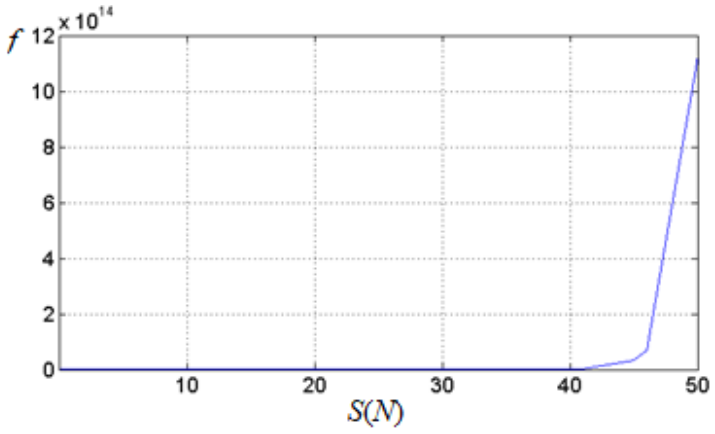


Рис. 5. График функции криптографической стойкости $f = 2^{S(N)}$

Отметим, что константа C определяет «эффективный» размер ключа, при котором начинается неограниченный рост функции. Это позволяет сделать выводы о достаточной криптографической стойкости КРК BB84 и его устойчивости к атакам типа brute force, поскольку полученные в ходе математического моделирования значения чрезвычайно велики и время их полного перебора существенно больше времени ценности информации.

Литература

[1] Авдошин С. *Дискретная математика. Модулярная алгебра, криптография, кодирование*. Москва, СИНТЕГ, 2016, 260 с.

[2] Адаменко М. *Основы классической криптологии. Секреты шифров и кодов*. Москва, Машиностроение, 2014, 256 с.

[3] Ассанж Дж. *Шифропанки: свобода и будущее Интернета*. Москва, Азбука-Аттикус, 2014, 574 с.

[4] Холево А.С. *Квантовые системы, каналы, информация*. Москва, МЦНМО, 2010, 328 с.

[5] Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. *Основы криптографии*. Москва, Гелиос АРВ, 2002, 480 с.

[6] Шнайер Б. Прикладная криптография. Москва, Триумф, 2002, 816 с.

[7] Bennett C.H., Brassard G. Quantum cryptography: public key distribution and coin tossing. *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, 1984, vol. 175, p. 8.

[8] Bennett C.H. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 1992, vol. 68, no. 21, pp. 3121–3124.

[9] Bennett C.H., Bessette F., Brassard G., et al. Experimental quantum cryptography. *Journal of Cryptology*, 1992, vol. 5, no. 1, pp. 3–28.

[10] Brassard G., Lutkenhaus N., Mor T., Sanders B.C. Limitations on practical quantum cryptography. *Physical Review Letters*, 2000, vol. 85, no. 6, pp. 1130–1133.

[11] Молотков С.Н. О коллективной атаке на ключ в квантовой криптографии на двух неортогональных состояниях. *Письма в ЖЭТФ*, 2004, т. 80, № 8, с. 639–644.

[12] Молотков С.Н. О предельных возможностях квантового распределения ключей с контролем статистики неоднофотонного источника. *Письма в ЖЭТФ*, 2008, т. 87, № 10, с. 674–679.

[13] Молотков С.Н. Квантовое распределение ключей с детерминистическим приготовлением и измерением квантовых состояний. *Письма в ЖЭТФ*, 2010, т. 91, № 1, с. 51–57.

[14] Федоров А.К. Современное состояние квантовой криптографии. *Студенческий научный вестник. Сб. тезисов общеуниверситетской науч.-тех. конф. «Студенческая научная весна — 2011»*. Т. X. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2012, с. 81–83.

[15] Федоров А.К. Противодействие атаке “Photon number splitting attack” при квантовом распределении ключа BB84. Студенческий научный вестник. *Сб. тезисов общеуниверситетской науч.-тех. конф. «Студенческая научная весна-2011»*. Т. XI, ч. II. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2012, с. 204–205.

Череданова Екатерина Максимовна — студентка кафедры «Защита информации», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Мамченко Елизавета Андреевна — студентка кафедры «Защита информации», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Марчук Александр Михайлович — студент кафедры «Робототехнические системы и мехатроника», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Речкунов Артем Андреевич — студент кафедры «Инновационное предпринимательство», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

MATHEMATICAL SIMULATION OF QUANTUM PROTOCOL BB84 KEY DISTRIBUTION

E.M. Cheredanova pankooova@mail.ru
SPIN-code: 1619-5499

E.A. Mamchenko liza.98.98@mail.ru
SPIN-code: 2887-3715

A.M. Marchuk marchuk.sasha2010@yandex.ru
SPIN-code: 9253-5492

A.A. Rechkunov recha.art@mail.ru
SPIN-code: 5018-1702

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The objective of this research is a mathematical simulation of quantum protocol bb84 key distribution in the MATLAB environment and evaluation of the cryptographic robustness of the transmitted data and its resistance to the attacks of the exhaustive values enumeration (such as the brute-force attack). Message passing through the quantum communication channel is carried out by means of generating random bit vectors, which demonstrate the choice of the polarization and measurement bases as well as the key agreement process through the conventional communication channel. Obtained during the mathematical simulation, the number of possible values subjected to the exhaustive enumeration, is immensely large, and the time for the enumeration of such values turned out to be more than the term of relevancy and importance of the intercepted information. The purpose of this work is to investigate the cryptographic robustness of quantum protocol bb84 key distribution and its resistance to the attacks such as the brute-force.

Keywords

Cryptography, quantum cryptography, encryption, protocol bb84, quantum key distribution, cryptographic robustness, Heisenberg indeterminacy principle

References

[1] Avdoshin S. Diskretnaya matematika. Modulyarnaya algebra, kriptografiya, kodirovanie [Discrete math. Modular algebra, cryptography, encoding]. Moscow, SINTEG publ., 2016, 260 p.

[2] Adamenko M. Osnovy klassicheskoy kriptologii. Sekrety shifrov i kodov [Fundamentals of classic cryptology. Secrets of ciphers and codes]. Moscow, Mashinostroenie publ., 2014, 256 p.

[3] Assange J. Cypherpunks: freedom and the future of the Internet. OR Books, 2016, 196 p. (Russ. ed.: Shifropanki: svoboda i budushchee Interneta. Moscow, Azbuka-Attikus publ., 2014, 574 p.)

[4] Kholevo A.S. Kvantovye sistemy, kanaly, informatsiya [Quantum systems, channels, information]. Moscow, MTsNMO publ., 2010, 328 p.

[5] Alferov A.P., Zubov A.Yu., Kuz'min A.S., Cheremushkin A.V. Osnovy kriptografii [Fundamentals of cryptography]. Moscow, Gelios ARV publ., 2002, 480 p.
[6] Schneier B. Applied cryptography: protocols, algorithms, and source code in C. Wiley, 1994, 618 p. (Russ. ed.: Prikladnaya kriptografiya. Moscow, Triumf publ., 2002, 816 p.)
[7] Bennett C.H., Brassard G. Quantum cryptography: public key distribution and coin tossing. *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, 1984, vol. 175, p. 8.
[8] Bennett C.H. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 1992, vol. 68, no. 21, pp. 3121–3124.
[9] Bennett C.H., Bessette F., Brassard G., et al. Experimental quantum cryptography. *Journal of Cryptology*, 1992, vol. 5, no. 1, pp. 3–28.
[10] Brassard G., Lutkenhaus N., Mor T., Sanders B.C. Limitations on practical quantum cryptography. *Physical Review Letters*, 2000, vol. 85, no. 6, pp. 1130–1133.
[11] Molotkov S.N. On a collective attack on the key in quantum cryptography on two nonorthogonal states. *Pis'ma v ZhETF*, 2004, vol. 80, no. 8, pp. 639–644. (Eng. version: *Journal of Experimental and Theoretical Physics Letters*, 2004, vol. 80, no. 8, pp. 563–567).
[12] Molotkov S.N. On the ultimate capabilities of the quantum key distribution with the control over the statistics of a non-single-photon source. *Pis'ma v ZhETF*, 2008, vol. 87, no. 10, pp. 674–679. (Eng. version: *Journal of Experimental and Theoretical Physics Letters*, 2008, vol. 87, no. 10, pp. 586–591.)
[13] Molotkov S.N. Quantum key distribution with the deterministic preparation and detection of quantum states. *Pis'ma v ZhETF*, 2010, vol. 91, no. 1, pp. 51–57. (Eng. version: *Journal of Experimental and Theoretical Physics Letters*, 2010, 91:1, 48–53.)
[14] Fedorov A.K. Sovremennoe sostoyanie kvantovoy kriptografii [Contemporary state of quantum cryptography]. *Studencheskiy nauchnyy vestnik. Sb. tezisov obshcheuniversitetskoy nauch.-tekh. konf. "Studencheskaya nauchnaya vesna – 2011". T. X* [Students science bulletin. Proc. Universiry Sci.-Tech. Conf "Students scientific spring-2011". Vol. X]. Moscow, Bauman Press, 2012, pp. 81–83.
[15] Fedorov A.K. Protivodeystvie atake "Photon number splitting attack" pri kvantovom raspredelenii klyucha BB84 ["Photon number splitting attack" resistance at quantum distribution of BB84 key]. *Studencheskiy nauchnyy vestnik. Sb. tezisov obshcheuniversitetskoy nauch.-tekh. konf. "Studencheskaya nauchnaya vesna — 2011". T. XI, ch. II* [Students science bulletin. Proc. Universiry Sci.-Tech. Conf "Students scientific spring-2011". Vol. XI. P. II]. Moscow, Bauman Press, 2012, pp. 204–205.

Cheredanova E.M. — student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Mamchenko E.A. — student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Marchuk A.M. — student, Department of Robotics and Mechatronics, Bauman Moscow State Technical University, Moscow, Russian Federation.

Rechkunov A.A. — student, Department of Innovative Entrepreneurship, Bauman Moscow State Technical University, Moscow, Russian Federation.