УДК 003.26 DOI:10.31854/1813-324X-2020-6-4-70-79

Система поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей. Часть 1. Алгоритм принятия решений

А.В. Власенко[1], **М.В. Евсюков**[1], **М.М. Путято**[1], **А.С. Макарян**[1]

[1]Кубанский государственный технологический университет,
Краснодар, 350072, Российская Федерация
*Адрес для переписки: putyato.m@gmail.com

Информация о статье
Поступила в редакцию 21.09.2020
Принята к публикации 22.10.2020.

Ссылка для цитирования: Власенко А.В., Евсюков М.В., Путято М.М., Макарян А.С. Система поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 70–79. DOI:10.31854/1813-324X-2020-6-4-70-79

Аннотация: *Цель данного исследования – разработка системы поддержки принятия решений (СППР), которая позволит для заданных условий применения криптосистемы выбрать наиболее подходящую реализацию постквантового механизма инкапсуляции ключей. В первой части цикла статей задача выбора оптимальной реализации постквантового механизма инкапсуляции ключей представлена как многокритериальная. Определены методы принятия решения, которые наиболее применимы к рассматриваемой задаче. Синтезирован алгоритм работы СППР и спроектировано веб-приложение, реализующее ее функционал.*

Ключевые слова: *квантовый компьютер, информационная безопасность, постквантовая криптография, механизм инкапсуляции ключей, принятие решений, метод последовательных уступок, веб-приложение.*

Введение

В последние годы наблюдается стремительный прогресс в области разработки квантовых компьютеров – вычислительных устройств, использующих квантовые явления запутанности и суперпозиции для хранения и обработки информации. Эксплуатация данных физических явлений позволяет квантовым компьютерам демонстрировать экспоненциально большую производительность по сравнению с классическими компьютерами при решении некоторых видов задач [1].

Как известно, безопасность наиболее распространенных на данный момент асимметричных криптосистем опирается на вычислительную сложность задач факторизации и дискретного логарифмирования [2]. В связи с этим значительное влияние на криптографию оказывает квантовый алгоритм Шора, позволяющий выполнять решение данных задач с полиномиальной сложностью [3]. Практическим следствием эффективности алгоритма Шора является полная неспособность информационных систем, использующих современную асимметричную криптографию, противостоять угрозе взлома при помощи квантового компьютера.

Данная уязвимость широко используемых асимметричных криптосистем потребовала создания алгоритмов нового поколения, способных эффективно противостоять квантовому криптоанализу. В результате такие криптосистемы стали называться постквантовыми, а алгоритмы, основанные на сложности задач факторизации и дискретного логарифмирования, – классическими [4].

Оценивается, что для разработки полноценного квантового компьютера потребуется около 10 лет [5]. В связи с этим Национальный институт стандартов и технологий США (NIST, *аббр. от англ.* National Institute of Standards and Technology) в 2016 г. начал процесс выбора алгоритмов на роль постквантовых криптографических стандартов электронно-цифровой подписи, шифрования с открытым ключом и механизма инкапсуляции ключей (МИК). Стандарты NIST имеют определяющее значение для криптографии во всем мире, поскольку многие международные организации, включая крупные банки и удостоверяющие центры инфраструктуры открытых ключей, используют криптографические алгоритмы, стандартизованные NIST.

Процедура выбора и утверждения криптографических стандартов проводится NIST в форме прозрачного, открытого для заявок и комментариев соревнования. Всего на конкурс потенциальных постквантовых стандартов были поданы 82 заявки, 69 из которых удовлетворили основным требованиям NIST и были допущены в первый тур. Во второй тур конкурса успешно прошли 26 кандидатов, 17 из которых – алгоритмы асимметричного шифрования и инкапсуляции ключей, а 9 – схемы цифровой подписи [6].

В ходе первых двух туров конкурса NIST заявителям удалось усовершенствовать предложенные алгоритмы, а научному сообществу – подробно исследовать кандидатов, оценить их безопасность, производительность, а также применимость к различным сценариям использования.

В результате второго тура конкурса 16 алгоритмов прошли в третий тур. Оставшиеся в конкурсе кандидаты были разделены на 2 группы: «финалисты конкурса» и «альтернативные кандидаты», которые являются потенциальными кандидатами для будущих процессов стандартизации [7].

Несмотря на то, что задача NIST – выбрать определенные алгоритмы в качестве стандарта, в своих отчетах институт подчеркивает полезность дифференцированного подхода к выбору используемой криптосистемы. В зависимости от особенностей защищаемого канала связи, предпочтительным может быть использование алгоритма, отличного от того, который закреплен в стандарте [8].

Постановка задачи

Цель данного исследования – разработка системы поддержки принятия решений, которая позволит для заданных условий применения средства защиты выбрать наиболее подходящую реализацию постквантового криптографического алгоритма.

В рамках данного исследования предполагается сконцентрироваться на задаче выбора оптимального МИК, в связи со следующими причинами:

– МИК реализует наиболее востребованную функцию асимметричной криптографии – безопасную доставку ключевого материала для алгоритма шифрования с закрытым ключом;

– среди представленных в конкурсе NIST кандидатов большая часть криптосистем являются именно МИК [6], что, с одной стороны, усложняет выбор оптимального алгоритма, а с другой – предоставляет достаточно большое пространство оптимизации, чтобы сделать эффективным дифференцированный подход.

Обоснование преимуществ предлагаемого подхода

Оценка эффективности и сравнение постквантовых криптографических алгоритмов – важные задачи современной криптологии, о чем свидетельствует большое количество научных работ, посвященных данной теме [4, 9, 10]. При этом, в большинстве исследований проводится прямое сравнение характеристик алгоритмов между собой с целью поиска лучшей криптосистемы. Преимущество такого подхода заключается в том, что он позволяет исследовать достоинства, недостатки, а также особенности применения криптосистем. В то же время существует ряд факторов, свидетельствующих об актуальности иного подхода к решению задачи выбора оптимального постквантового криптографического алгоритма, а именно – подхода, ориентированного на свойства и требования защищаемой информационной системы.

Во-первых, в ходе процесса стандартизации было выявлено большое количество алгоритмов, которые отвечают базовым требованиям производительности и достаточно безопасны для того, чтобы их можно было использовать на практике. Более того, они демонстрируют значительную вариативность характеристик от алгоритма к алгоритму, что предоставляет потенциальному пользователю широкое разнообразие альтернатив для выбора средства обеспечения информационной безопасности, которое наиболее полно отвечает требованиям объекта защиты [6].

Во-вторых, для каждого из представленных заявителями кандидатов существует несколько реализаций, каждая из которых задает собственный баланс между метриками безопасности и эффективности. Так, например, алгоритм «Round5» имеет 5 различных реализаций уровня безопасности AES-128 [11]. Данный фактор позволяет пользователю определить наиболее подходящую под требования конкретной информационной системы реализацию алгоритма. В дополнение к предыдущему фактору это значительно увеличивает количество и разнообразие альтернатив, доступных пользователю.

В-третьих, существует большое количество сценариев применения, в которых использование криптографии не попадает под строгие законодательные регуляции. Следовательно, становится целесообразным рассмотрение возможности эксплуатации алгоритмов, которые не закреплены в стандарте NIST, поскольку некоторые из них могут оказаться более предпочтительными при использовании для защиты конкретной информационной системы.

В-четвертых, изучение способности конкретных реализаций МИК соответствовать требованиям различных сценариев использования представляет исследовательскую ценность. Данные сведения важны для будущих процессов стандартизации, в частности, при принятии специальных стандартов, ориентированных на информационные системы определенного рода, а также локальных государственных стандартов, например, российских.

Описание задачи выбора оптимальной реализации постквантового МИК в терминологии теории принятия решений

Для решения задачи выбора оптимальной реализации постквантового МИК целесообразно воспользоваться теорией принятия решений.

Теория принятия решений – математическая дисциплина, изучающая методы эффективного поиска оптимальной альтернативы из доступного множества [12].

Частным случаем общей задачи принятия решения является задача многокритериального выбора. Данная задача состоит из следующих компонентов:

– $A = \{a_1, \dots, a_n\}$ – конечное множество допустимых решений, из которого требуется выбрать одну или несколько альтернатив, в наибольшей мере соответствующих предъявляемым требованиям;

– $X = \{x_1, \dots, x_m\}$ – конечное множество критериев оценки, т. е. совокупность значимых для конкретной задачи принятия решения характеристик рассматриваемых альтернатив;

– $a_i(X) = \{a_i(x_1), \dots, a_i(x_m)\}$, где $i = \overline{1,n}$ – векторные оценки каждой альтернативы по каждому критерию из множества X;

– $R = \{R_{x_1}, \dots, R_{x_m}\}$ – множество бинарных отношений предпочтения «не хуже», определенное для значений каждого критерия $x \in X$ и позволяющее путем сравнения пары значений определить не менее предпочтительное из них; например, для $h, k \in x$, если hR_xk, то значение h критерия x не хуже значения k; данные отношения обладают свойствами рефлексивности:

$$\forall h \in x \; hR_xh, \tag{1}$$

а также транзитивности:

$$\forall h, k, l \in x \; hR_xk \wedge kR_xl \implies hR_xl. \tag{2}$$

Кроме того, в рамках рассматриваемой задачи, для удобства дальнейших рассуждений целесообразно наложить следующие ограничения на отношения предпочтения:

– множество значений любого критерия x является линейно упорядоченным;

– каждое отношение R_x является отношением строгого порядка над множеством соответствующего ему критерия x:

$$\forall h, k \in x \; hR_xk \vee kR_xh, \tag{3}$$

из этого также следует, что отношение R_x антисимметрично:

$$\forall h, k \in x \; hR_xk \wedge kR_xh \iff k = h, \tag{4}$$

для удобства, будет использовано бинарное отношение «строго лучше» R_x^s, которое выполняется, для неравных значений критерия находящихся в отношении R_x (R_x^s – нерефлексивная версия отношения «не хуже»).

Таким образом, представление задачи выбора оптимальной реализации постквантового МИК для заданных условий применения в терминологии теории принятия решений принимает следующий вид:

– в роли множества альтернатив A выступает множество из 91 реализаций постквантовых МИК, признанных безопасными в результате первого этапа конкурса NIST [7];

– в роли множества X критериев оценки выступает система критериев, предложенная в исследовании [13];

– в роли векторной оценки некоторого МИК $a_i(X)$ по списку критериев X выступают значения замеров производительности [14] количественных параметров и формализованные качественные характеристики, представленные в числовой форме;

– в роли бинарного отношения «не хуже» R_x для количественных критериев, таких как длина открытого ключа, выступает отношение «меньше или равно» (меньшая длина ключа предпочтительнее большей); для качественных критериев, таких как надежность, используется отношение «больше или равно» (бóльшая надежность предпочтительнее меньшей);

– в роли бинарного отношения «строго лучше» R_x^s, соответственно, выступают отношения «меньше» или «больше», в зависимости от рассматриваемого критерия x.

Система критериев оценки постквантовых МИК

Как было отмечено выше, важной составляющей задачи принятия решения является множество критериев, используемых для оценки и сравнения альтернатив. В данном разделе приводится краткое изложение системы критериев оценки постквантовых МИК, сформулированных в исследовании [13]:

1) безопасность:

– *изученность* математической задачи, вычислительная сложность решения которой обеспечивает надежность криптосистемы; характеристика отражает временной срок, на протяжении которого математический аппарат, используемый криптосистемой, изучается в качестве механизма обеспечения криптографической стойкости: *задачи, предложенные более 20, более 10, менее 10 лет назад*;

– *доказательство* или убедительность теоретического обоснования надежности схемы; качество доказательства криптографической стойкости алгоритма вносит не меньший вклад в обеспечение уверенности в безопасности криптосистемы, чем выбор математического аппарата: *одно из наиболее убедительных доказательств; доказательство не содержит суждений, которые оцени-*

ваются экспертами NIST, как сомнительные; доказательство содержит суждения, истинность которых не вызывают у экспертов NIST полной уверенности;

– *устойчивость МИК* – тип криптоаналитических атак, к которым устойчив МИК: *устойчивость к атакам на основе подобранного шифртекста; устойчивость к атакам на основе подобранного открытого текста*;

2) ресурсоемкость:

– *размер открытого ключа;*

– *размер шифртекста;*

– *производительность инкапсуляции* – вычислительная эффективность операции зашифрования передаваемого симметричного ключа в циклах работы процессора;

– *производительность декапсуляции* – вычислительная эффективность операции расшифрования передаваемого симметричного ключа в циклах работы процессора;

– *производительность генерации пары ключей* – вычислительная эффективность операции расшифрования передаваемого симметричного ключа в циклах работы процессора.

Далее следует провести оценку каждой альтернативы, воспользовавшись выделенной системой критериев. Источником информации о производительности реализаций служат бенчмарки, выполненные различными группами исследователей [14]. Сведения о безопасности и гибкости реализаций получены в результате изучения комментариев NIST о заявках [6, 8, 11], а также информации об алгоритмах, предоставленной заявителями [12].

Для того, чтобы сведения о безопасности реализаций было возможно использовать в математических методах принятия решения, их необходимо привести к числовой форме. Поскольку такие свойства, как убедительность доказательства и изученность математического аппарата характеризуют степень доверия к предположению безопасности, на котором основана криптосистема, целесообразно консолидировать их в один параметр.

Применяемый способ формализации частных критериев «Изученность сложной задачи» и «Убедительность доказательства» приведен в таблице 1. Полученный числовой параметр называется «Доверие».

ТАБЛИЦА 1. Создание числового параметра «Доверие»

TABLE 1. Creating Numeral Parameter "Trust"

Изученность сложной задачи	Убедительность доказательства	Доверие
Консервативная	Отлично	6
Зрелая	Отлично	5
Зрелая	Хорошо	4
Зрелая	Требуются исследования	3
Новая	Хорошо	2
Новая	Требуются исследования	1

На основе общедоступной информации сформирована база данных о 91 реализации постквантовых МИК, прошедших во второй этап конкурса NIST, представленная в форме файла формата json. При этом, в структуру объекта json включены следующие поля:

«name» – название реализации;

«submission» – название заявки (алгоритма);

«subproblem» – разновидность сложной задачи реализацией;

«genAvg» – средние затраты на генерацию пары ключей;

«encAvg» – средние затраты на инкапсуляцию;

«decAvg» – средние затраты на декапсуляцию;

«sk» – длина секретного ключа;

«pk» – длина открытого ключа;

«ct» – длина шифртекста;

«securityLevel» – уровень безопасности реализации;

«ind» – разновидность защищенности от криптоанализа;

«trust» – упрощенная характеристика надежности, которая учитывает только изученность сложной задачи реализации;

«trustDetailed» – числовой параметр «доверие»;

«id» – уникальный идентификатор реализации в базе данных.

Поиск множества Парето-оптимальных альтернатив

В качестве первого шага алгоритма работы проектируемой советующей системы целесообразно выбрать один из наиболее широко используемых инструментов теории принятия решений, а именно понятие Парето-оптимальности.

Для выделения подмножества альтернатив, выбор которых является оптимальным в смысле Парето, вводится понятие бинарного отношения доминирования D на множестве альтернатив A [15].

Говорят, что альтернатива a_1 доминирует альтернативу a_2 по Парето, если оценки альтернативы a_1 по всем частным критериям не хуже, чем у a_2 и строго лучше хотя бы по одному критерию:

$$a_1 D a_2 \Leftrightarrow [\forall x \in X\ a_1(x) R_x a_2(x)] \wedge \left[\exists y \in X\ a_1(y) R_y^s a_2(y)\right]. \quad (5)$$

Действительно, если a_1 и a_2 находятся в отношении доминирования (именно в таком порядке), то выбор альтернативы a_1 более предпочтителен, чем выбор альтернативы a_2. Тогда, используя данное отношение, из множества альтернатив A можно выделить подмножество $A^{\text{нд}}$ тех альтернатив, которые не доминируются никакой другой альтернативой:

$$A^{\text{нд}} = \{a \in A | \nexists b \in A\ bDa\}. \quad (6)$$

Принцип оптимальности Парето утверждает, что рациональным является выбор любой альтернативы, входящей в множество $A^{\text{нд}}$. Множество $A^{\text{нд}}$

построено таким образом, что в него включены только те элементы области выбора, для которых не нашлось строго лучшей альтернативы [15].

Тем не менее, использование принципа оптимальности Парето зачастую недостаточно для принятия обоснованного решения. Во-первых, при большом порядке исходного множества A, множество $A^{нд}$, как правило, также оказывается слишком большим, чтобы его можно было считать успешным решением задачи оптимального выбора. Во-вторых, при сравнении двух произвольных альтернатив из множества $A^{нд}$ друг с другом, каждая из них будет превосходить другую, как минимум, по одному параметру.

В связи с этим, после применения принципа оптимальности Парето требуется использование методов, учитывающих приоритет частных критериев, обусловленный условиями задачи.

Адаптация метода последовательных уступок под особенности задачи выбора оптимальной реализации МИК

В качестве основного метода принятия решения выбран метод последовательных уступок (далее – МПУ) [15], поскольку он обладает следующими преимуществами:

– позволяет принять во внимание все частные критерии, с учетом их приоритета;

– обеспечивает возможность компенсации значений одних критериев значениями других таким образом, чтобы это приводило к повышению общей оптимальности решения;

– позволяет использовать нечеткие данные для описания задачи.

МПУ применим в тех случаях, когда допустимо снижение оптимальности значений более важных критериев, в пользу повышения значений менее важных [15].

При использовании МПУ для описания требований конкретной задачи к характеристикам альтернатив выполняются следующие действия:

– частные критерии сортируются в порядке убывания их приоритета: наиболее важный критерий становится первым, а наименее важный – последним;

– для каждого критерия (кроме последнего) определяется размер уступки, которую допустимо совершить с целью улучшения значений менее приоритетных критериев.

После описания требований задачи происходит поиск лучшего решения по наиболее важному критерию. Затем ищется лучшее решение по следующему приоритному критерию, при этом допускается потеря от лучшего значения первого критерия не более, чем на определенную величину, т. е. делается уступка. На третьем шаге решение оптимизируется по третьему критерию, при заданных максимальных допустимых уступках по первому и второму критериям и т. д., пока не будет рассмотрен последний по важности критерий [15].

Важно заметить, что эффективное решение задачи выбора оптимального МИК не может быть ограничено рассмотрением таких просто формализуемых характеристик алгоритмов, как безопасность и производительность. Необходимо также учесть особенности алгоритмов, характеризующие гибкость их применения. В качестве примеров гибкости выступают возможность легкого встраивания алгоритма в существующие приложения, простота регулирования характеристик криптосистемы путем изменения ее параметров, а также другие особенности, которые не представляется возможным принять во внимание в рамках математических методов принятия решения.

Поскольку МПУ в его оригинальной форме нацелен на выбор единственной лучшей альтернативы [15], оптимальное, согласно методу, решение будет выбрано без учета неформализованных свойств алгоритма. Это может быть неприемлемо для лица, принимающего решение, поэтому МПУ целесообразно использовать не для выбора единственной оптимальной альтернативы, а для составления рейтинга лучших альтернатив по безопасности и производительности. Информацию о неформализованных свойствах алгоритма при разработке системы поддержки принятия решения в таком случае можно донести до лица, принимающего решение, в форме справочной информации.

Для повышения эффективности МПУ, применительно к рассматриваемой задаче, предлагается внести в него две модификации.

Во-первых, алгоритм будет выполняться итерационно. На каждой итерации, при помощи МПУ, в множестве Парето-оптимальных альтернатив находится наиболее оптимальное решение. Затем оно помещается в конец рейтинга решений и исключается из множества альтернатив. Алгоритм повторяется до тех пор, пока в множестве альтернатив не останется последний элемент.

Во-вторых, будет видоизменен сам механизм уступки. Пусть альтернатива b имеет худшее значение более приоритетного критерия x, но лучшее значение менее приоритетного критерия y по сравнению с альтернативой a. Тогда альтернатива b будет считаться более предпочтительной, чем альтернатива a при выполнении следующих условий:

– разность между $a(x)$ и $b(x)$ не превышает размер уступки, установленной для критерия x;

– разность между $b(y)$ и $a(y)$ больше, чем размер уступки, установленной для критерия y.

Иными словами, сравнение альтернатив происходит с учетом отношения безразличия, которое задается для каждого критерия его уступкой.

Алгоритм работы системы поддержки принятия решений

Описанные в предыдущих разделах аспекты задачи выбора оптимального постквантового МИК позволяют сконструировать алгоритм работы системы поддержки принятия решений, который состоит из следующих шагов.

Шаг 1. Ввод пользователем параметров, описывающих условия использования криптосистемы.

*Шаг 2. В*ыбор из базы данных реализаций, предоставляющих требуемый уровень криптографической защиты.

Шаг 3. Фильтрация выбранных реализаций по соответствию целевому способу управления закрытым и открытым ключами.

Шаг 4. Нахождение множества Парето-оптимальных альтернатив.

Шаг 5. Определение приоритета частных критериев и размеров их уступок, в зависимости от введенного пользователем описания условий информационного взаимодействия.

Шаг 6. Применение адаптированного МПУ для построения рейтинга альтернатив.

Шаг 7. Вывод рейтинга реализаций постквантовых МИК, отсортированных в порядке убывания оптимальности по критериям «безопасность» и «производительность».

Кроме того, в системе поддержки принятия решения будет предусмотрена возможность ознакомления со справочной информацией об алгоритмах, включенных в рейтинг.

Пользовательский интерфейс системы поддержки принятия решений

Обоснованность рекомендаций системы поддержки принятия решений напрямую зависит от подробности описания условий применения криптографического алгоритма. В связи с этим необходимо выделить набор параметров, совокупность которых позволит достаточно точно смоделировать свойства ИС-абонентов и характер их взаимодействия. В то же время, важно не перегружать интерфейс избыточным количеством входных параметров, чтобы обеспечить его дружелюбность по отношению к пользователю.

Минимальная версия входного интерфейса приложения содержит следующие параметры.

Сценарий взаимодействия.

1) Формат связи: веб-сайт (протокол TLS с односторонней аутентификацией); VPN (протокол IPsec); приложение банка (протокол TLS с взаимной аутентификацией); мессенджер (протокол Signal).

2) Способ управления парой ключей: ключи не используются повторно; ключи используются повторно и открытый ключ не кешируется на стороне клиента; ключи используются повторно и открытый ключ кешируется на стороне клиента.

Характеристики целевого клиента.

1) Мощность клиента: смартфон; ноутбук; настольный компьютер.

2) Пропускная способность канала связи: низкая; средняя; высокая.

Характеристики целевого сервера.

1) Мощность сервера: смартфон; ноутбук; настольный компьютер.

2) Количество одновременных подключений: низкое; среднее; высокое.

Требуемый уровень безопасности соединения: AES-128; AES-256; AES-512.

Приведенная система входных параметров, описывающих информационное взаимодействие, представляется минимальной и поддерживает возможность детализации и расширения. Ввод формата связи позволяет определить используемый в ходе информационного обмена протокол. На подготовительном этапе адаптированного МПУ именно для конкретных протоколов определяется приоритет частных критериев и допустимые размеры уступок.

В целях упрощения интерфейса, рассматриваемые в рамках системы поддержки принятия решений разновидности вычислительных устройств, выступающих в роли клиентов и серверов, разделены на несколько условных категорий (в порядке увеличения производительности): смарткарта (токен); устройство интернета вещей; смартфон; микрокомпьютер; ноутбук; настольный компьютер; промышленный сервер.

Аналогично количество подключений к серверу также определено в словесной форме. Однако предполагается указывать конкретное число подключений в интерфейсе ввода, в зависимости от мощности сервера. Интерфейс вывода рейтинга реализаций МИК и справочной информации – на рисунке 1.

Принцип определения приоритета критериев и размеров уступок при использовании адаптированного МПУ

Важнейшим аспектом использования МПУ является выбор приоритета частных критериев и размеров допустимых уступок. Именно на основании этих параметров делается вывод о предпочтительности той или иной альтернативы [15]. В данном разделе описывается принцип подбора этих параметров, в зависимости от данных, введенных пользователем.

С точки зрения абонентов, свойства канала связи, защищаемого при помощи криптографии, можно смоделировать, используя следующие метрики: безопасность канала связи; затраты на клиентские вычисления; затраты на серверные вычисления; затраты на передачу данных во время выполнения протокола.

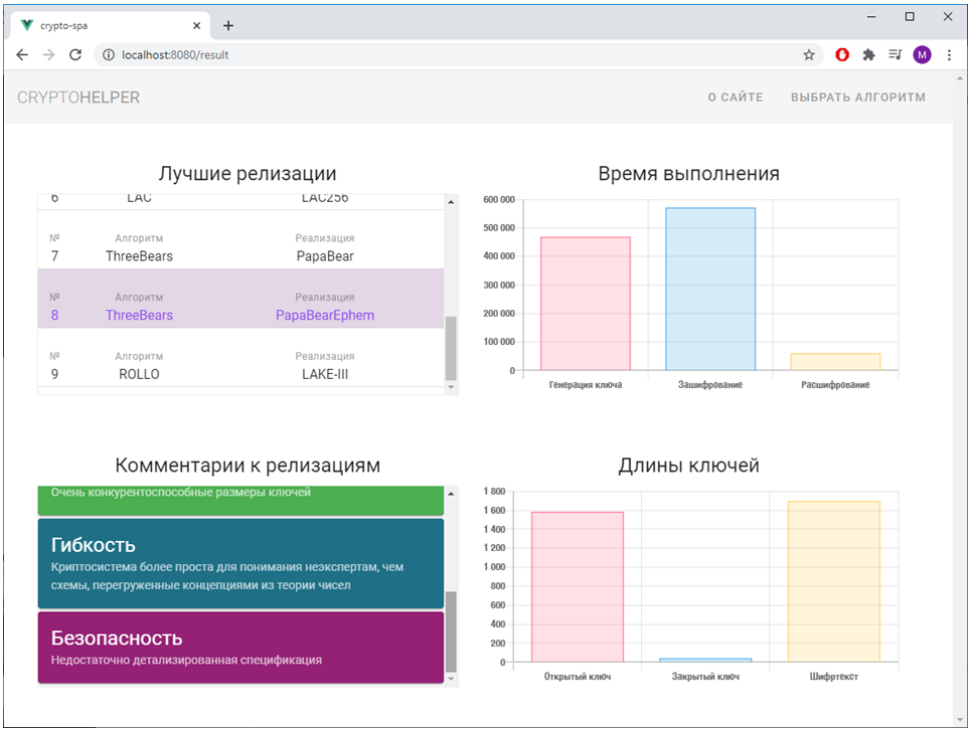

Рис. 1. Интерфейс вывода рейтинга реализаций МИК

Fig. 1. Implementation Rating Output Interface

Первая метрика из перечисленных отражает качество связи, а остальные – временные затраты на выполнение сеанса протокола. Именно эти метрики предполагается использовать в качестве частных критериев в МПУ. Таким образом, при подготовке информации для адаптированного МПУ, в зависимости от условий применения алгоритма, введенных пользователем, необходимо определить комбинацию характеристик постквантовых МИК, которая сможет служить в качестве значения для каждой из метрик канала связи.

В таблице 2 приведен используемый способ выразить метрики канала связи через характеристики реализаций постквантовых МИК в зависимости от способа управления ключами.

ТАБЛИЦА 2. Выражение метрик канала связи через свойства МИК

TABLE 2. Representing Datachannel Metrics via KEM's Properties

Метрика канала связи	Ключи не используются повторно	Ключи используются повторно	
		без кеширования на стороне клиента	с кешированием на стороне клиента
Безопасность	«trustDetailed» – для 3-го уровня безопасности, «trust» – в остальных случаях		
Клиентские вычисления	«encAvg»		
Серверные вычисления	«decAvg» + «genAvg»	«decAvg», «genAvg»	
Передача данных	«pk» + «ct»		«ct», «pk»

В данной таблице символ «+» означает сложение значений характеристик, а символ «,» значит, что характеристики учитываются отдельно, как разные частные критерии. Таким образом, МПУ оперирует наибольшим числом критериев при повторном использовании ключей с кешированием на стороне клиента. Это связано с тем, что в таком случае генерация пары ключей сервером и передача открытого ключа клиенту происходят не в каждом сеансе протокола. Несмотря на это, даже при таких условиях параметрами «pk» и «genAvg» не всегда можно пренебречь. Поэтому рациональным представляется их рассмотрение в МПУ, как второстепенных свойств реализаций, оказывающих меньшее влияние на метрики канала связи, чем «ct» и «decAvg».

Приоритет частных критериев и размеры уступок определяются путем выполнения последовательности проверок описания условий применения криптосистемы, введенного пользователем. Предполагается по результату каждой проверки поместить в массив специальный объект, описывающий приоритет некоторой метрики и размер допустимой уступки. Далее адаптированный МПУ будет использовать данный массив в качестве источника данных о частных критериях, избегая повторной оптимизации по каждой из четырех метрик канала связи. При сравнении пары альтернатив будет указан размер уступки относительно той альтернативы, которая обладает меньшим значением рассматриваемой характеристики.

Кроме того, в сигнатуру объекта, из экземпляров которого состоит массив, предполагается добавить специальное поле – показатель приоритета (используется при сортировке массива объектов для адаптированного МПУ). Меньший показатель

приоритета означает бóльшую важность оптимизируемой метрики.

В таблице 3 приведен пример последовательности условий, используемой для протокола TLS-handshake, применяемого без повторного использования ключей. Таблица является частным случаем общего набора условий для сценария применения, использующего TLS-handshake с односторонней аутентификацией, применяемого без повторного использования ключей. Поэтому последнее условие всегда является истинным. Тем не менее, его наличие в последовательности условий целесообразно, поскольку оно задает приоритет и уступки для метрик «Передача данных» и «Серверные вычисления» для случая, когда эти метрики не были покрыты предыдущими условиями.

ТАБЛИЦА 3. Последовательность условий для протокола TLS-Handshake

TABLE 3. Sequence of Conditions for TLS-Handshake Protocol

Условие	Метрика канала связи	Характеристики МИК	Размер уступки	Показатель приоритета
Требуемый уровень безопасности – AES3	Безопасность	«trustDetailed»	1 уровень	1
Высокая нагрузка на сервер	Серверные вычисления	«decAvg» + «genAvg»	30 %	Если мощность сервера не превосходит мощность клиента – 11, иначе – 13
	Передача данных	«pk» + «ct»	100 %	Если канал связи обладает малой пропускной способностью – 12, иначе – 14
Мощность сервера не превосходит мощность клиента	Серверные вычисления	«decAvg» + «genAvg»	30 %	21
Канал связи обладает малой пропускной способностью	Передача данных	«pk» + «ct»	100 %	31
Требуемый уровень безопасности – AES2	Безопасность	«trust»	1 уровень	41
Малая мощность вычислительного устройства клиента	Клиентские вычисления	«encAvg»	30 %	51
Низкая нагрузка на сервер	Клиентские вычисления	«encAvg»	30 %	61
	Безопасность	«trust»	1 уровень	62
Не допускается повторное использование ключей	Серверные вычисления	«decAvg» + «genAvg»	30 %	71
	Передача данных	«pk» + «ct»	100 %	72

Заключение

В ходе первой части исследования произведен выбор алгоритмов принятия решения для разрабатываемой системы, выполнена адаптация МПУ в соответствии с особенностями рассматриваемой задачи. В качестве частных критериев для МПУ предложено использовать метрики канала связи, которые затем выражены через характеристики МИК. Сформирована база данных характеристик существующих реализаций механизмов инкапсуляции ключей. Выполнена практическая реализация прототипа поддержки принятия решения в форме веб-приложения. Приведены доводы в пользу предлагаемого подхода к решению задачи выбора оптимального постквантового МИК.

Однако конкурентоспособность предложенного подхода требует научного обоснования. Для этого требуется провести практическую апробацию и оценку эффективности разработанной системы поддержки принятия решений с учетом существующих аналитических исследований в области постквантовой криптографии. Именно решению данных задач будет посвящена вторая часть цикла статей.

Список используемых источников

1. Гринштейн Д., Зайонц А. Квантовый вызов. Современные исследования оснований квантовой механики. М.: Изд-во Интеллект, 2012. 432 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Изд-во Триумф, 2002. 815 с.

3. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Review. 1999. Vol. 41. Iss. 2. PP. 303–332. DOI:10.1137/S0036144598347011

4. Комарова А.В., Коробейников А.Г. Анализ основных существующих пост-квантовых подходов и схем электронной подписи // Вопросы кибербезопасности. 2019. № 2(30). С. 58–68. DOI:10.21681/2311-3456-2019-2-58-68
5. Chen L., Jordan S., Liu Y., Moody D., Peralta R., Perlner R., et al. Report on Post Quantum Cryptography. Gaithersburg: NIST, 2016. 15 p. DOI:10.6028/NIST.IR.8105
6. Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Liu Y.-K., et al. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. Gaithersburg: NIST, 2019. 27 p. DOI:10.6028/NIST.IR.8240
7. Moody D. Round2 of the NIST PQC "Competition" what was NIST thinking? // The 10th International Conference on Post-Quantum Cryptography (PQCrypto 2019), Chongqing, China, 8–10 May 2019. URL: https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf (дата обращения 03.11.2020)
8. Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Kelsey J., et al. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. Gaithersburg: NIST, 2020. 39 p. DOI:10.6028/NIST.IR.8309
9. Луценко М.С., Киян А.С., Кузнецова Т.Ю., Кузнецов А.А. Анализ и сравнительные исследования кодовых схем инкапсуляции ключей, представленные на конкурсе NIST PQC // Всеукраинский межведомственный научно-технический сборник «Радиотехника». 2018. № 193. С. 66–53. URL: https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_193_8.pdf (дата обращения 14.09.2020)
10. Михайличенко Д.А., Егорова А.А. Основные направления развития постквантовой криптографии // Труды Ростовского государственного университета путей сообщения. 2016. № 2. С. 41–45.
11. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standartization Process // NIST. URL: https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf (дата обращения 03.11.2020)
12. Baan H., Bhattacharya S., Fluhrer S., Garcia-Morchon O., Laarhoven T., Player R., et al. Round5: KEM and PKE based on (Ring) Learning with Rounding // Round5 submission to NIST PQC standardization. URL: https://round5.org/doc/Round5_Submission042020.pdf (дата обращения 03.11.2020)
13. Власенко А.В., Евсюков М.В., Путято М.М., Макарян А.С. Исследование реализации механизмов инкапсуляции ключей постквантовых криптографических методов // Прикаспийский журнал: управление и высокие технологии. 2019. № 4(48). С. 121–127. DOI:10.21672/2074-1707.2019.48.4.121-127
14. Kannwischer M.J., Rijneveld J., Schwabe P., et al. Testing and Benchmarking NIST PQC on ARM Cortex-M4 // Radboud University. URL: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/kannwischer-pqm4.pdf (дата обращения 14.09.2020)
15. Горбунов В.М. Теория принятия решений: учебное пособие. Томск: Изд-во Национальный исследовательский Томский политехнический университет, 2010. 67 с.

* * *

Decision Support System for Finding an Optimal Postquantum Key Encapsulation Mechanism Part 1. Decision Making Algorithm

A. Vlasenko[1], **M. Evsyukov**[1], **M. Putyato**[1], **A. Makaryan**[1]

[1]Kuban State Technological University,
Krasnodar, 350072, Russian Federation

Article info
DOI:10.31854/1813-324X-2020-6-4-70-79
Received 21st September 2020
Accepted 22nd October 2020

For citation: Vlasenko A., Evsyukov M., Putyato M., Makaryan A. Decision Support System for Finding an Optimal Postquantum Key Encapsulation Mechanism. Part 1. Decision Making Algorithm. *Proc. of Telecom. Universities.* 2020;6(4):70–79. (in Russ.) DOI:10.31854/1813-324X-2020-6-4-70-79

Abstract: *The purpose of this study is to develop a decision support system that will allow, for the given conditions of using the cryptosystem, to choose the most appropriate implementation of the post-quantum key encapsulation mechanism. In the first part of the series of articles, the problem of choosing the optimal implementation of the post-quantum key encapsulation mechanism is presented as a multi-criteria choice problem. Decision-making methods that are best applicable to the problem under consideration have been determined. An algorithm for solving the problem has been developed. A web application has been designed that implements the functionality of a decision support system.*

Keywords: *quantum computer, information security, postquantum cryptography, key encapsulation mechanism, decision-making, asymmetric cryptography, web-application.*

References

1. Grinshteyn D., Zayonz A. *Quantum Challenge. Modern Research of Quantum Mechanic's Basics*. Moscow: Intellect Publ.; 2012. 432 p. (in Russ.)
2. Schneier B. *Applied Cryptography: Protocols, Algorthms, and Source Code*. Moscow: Triumph Publ.; 2002. 815 p. (in Russ.)
3. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*. 1999;41(2):303–332. DOI:10.1137/S0036144598347011
4. Komarova A.V., Korobeynikov A.G. The Analysis of Existing Post-Quantum Approaches and Electronic Signature Schemes. *Voprosy kiberbezopasnosti (Cybersecurity issues)*. 2019;2(3):58–68. (in Russ.) DOI:10.21681/2311-3456-2019-2-58-68
5. Chen L., Jordan S., Liu Y., Moody D., Peralta R., Perlner R., et al. *Report on Post Quantum Cryptography*. Gaithersburg: NIST; 2016. 15 p. DOI:10.6028/NIST.IR.8105
6. Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Liu Y.-K., et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. Gaithersburg: NIST; 2019. 27 p. DOI:10.6028/NIST.IR.8240
7. Moody D. Round2 of the NIST PQC "Competition" what was NIST thinking? *The 10th International Conference on Post-Quantum Cryptography (PQCrypto 2019), Chongqing, China, 8–10 May 2019*. Available from: https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf [Accessed 3nd November 2020]
8. Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Kelsey J., et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. Gaithersburg: NIST; 2020. 39 p. DOI:10.6028/NIST.IR.8309
9. Lucenko M.S., Kiyan A.S., Kuznetsova T.U., Kuznetsov A.A. Analysis and Comparative Studies of Key Encapsulation Code Schemes Presented in the Competition NIST PQC. *All-Ukrainian Interdepartmental Scientific and Technical Journal "Radiotehnika"*. 2018;193. (in Russ.) Available from: https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_193_8.pdf [Accessed 14th September 2020]
10. Mihaylichenko D.A., Egorova A.A. Main Areas of Post Quantum Cryptography. *Proceedings of the Rostov State Transport University*. 2016;2:41–45. (in Russ.)
11. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standartization Process. *NIST.* Available from: https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf [Accessed 3nd November 2020]
12. Baan H., Bhattacharya S., Fluhrer S., Garcia-Morchon O., Laarhoven T., Player R., et al. *Round5: KEM and PKE based on (Ring) Learning with Rounding*. Available from: https://round5.org/doc/Round5_Submission042020.pdf [Accessed 3nd November 2020]
13. Vlasenko A.V., Evsyukov M.V., Putyato M.M., Makaryan A.S. Research of Key Encapsulation Mechanisms Based on Postquantum Cryptographic Algorithms. *Caspian journal: Management and High Technologies*. 2019;4(48):121–127. (in Russ.) DOI:10.21672/2074-1707.2019.48.4.121-127
14. Kannwischer M.J., Rijneveld J., Schwabe P., et al. *Testing and Benchmarking NIST PQC on ARM Cortex-M4*. Available from: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/kannwischer-pqm4.pdf [Accessed 14th September 2020]
15. Gorbunov V.M. *Decision Theory*. Tomsk: Tomsk Polytechnic University Publ.; 2010. 67 p. (in Russ.)

Сведения об авторах:

ВЛАСЕНКО Александра Владимировна — кандидат технических наук, доцент, заведующая кафедрой «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, alex_vlasenko@list.ru

ЕВСЮКОВ Михаил Витальевич — аспирант кафедры «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, michael.evsyukov@gmail.com

ПУТЯТО Михаил Михайлович — кандидат технических наук, доцент, доцент кафедры «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, putyato.m@gmail.com

МАКАРЯН Александр Самвелович — кандидат технических наук, доцент, доцент кафедры «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, msanya@yandex.ru