ОТЗЫВ

официального оппонента

на диссертационную работу **Ахметзяновой Лилии Руслановны**

«Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации», представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

Как известно, наиболее трудным и ответственным этапом разработки любой криптографической конструкции является обоснование ее стойкости. Среди разнообразных подходов, используемых для этой цели, наиболее интересным с математической точки зрения является теоретико-доказательный подход. Он предполагает создание математической модели, в которой, помимо строгого описания анализируемой криптографической конструкции, формулируются описания информационной осведомленности и вычислительных возможностей противника (атака) и целевой функции (угроза). Оценки значений угрозы при всевозможных допустимых атаках определяют уровень стойкости рассматриваемой криптографической конструкции. Разработка, развитие и применение методов получения этих оценок является одним из наиболее важных направлений исследований математической криптографии.

Общие принципы построения указанных математических моделей для анализа стойкости криптографических схем хорошо известны. Однако их реализация и получение на их основе как можно более точных оценок уровня стойкости существенно зависит от разновидности криптографических конструкций; почти всегда это оказывается индивидуальной задачей, решение которой требует немалой изобретательности, математической сноровки и искусного владения аппаратом алгебры, комбинаторики, теории вероятности и теории сложности вычислений. Решению именно такой задачи для одного перспективного класса схем аутентифицированного шифрования с ассоциированными данными (AEAD-схем) посвящена диссертация Л.Р. Ахметзяновой.

AEAD-схема представляет собой пару соответствующих друг другу процедур шифрования-расшифрования, в которой процедура шифрования, используя единый секретный ключ, вычисляет не только криптограмму заданного

сообщения, но также и код аутентификации самого сообщения и некоторого ассоциированного с ним набора данных, который может оставаться при этом в незашифрованном виде. Схемы такого рода чрезвычайно востребованы, например, при передаче конфиденциальных данных в незащищенных телекоммуникационных сетях. По сравнению с традиционными задачами шифрования и электронно-цифровой подписи задача построения стойких AEAD-схем осложнена двумя факторами: 1) один и тот же секрет используется для обеспечения как конфиденциальности, так и целостности передаваемого сообщения, 2) целостность должна быть обеспечена как для зашифрованного сообщения, так и для ассоциированных с ним открытых данных. Другая особенность AEAD-схемы состоит в том, что одним из ее компонентов является алгоритм блочного симметричного шифрования (БСА), который служит «сменным модулем», и поэтому уровень стойкости AEAD-схем в математических моделях нужно рассматривать как функцию не только от параметров схемы и ограничений на вычислительные ресурсы противника, но также от уровня стойкости БСА. Алгоритм, являющийся окружением («оболочкой») БСА в AEAD-схемах, называется AEAD-режимом. Именно AEAD-режимы и методы оценки их уровня стойкости являются предметом исследований в диссертации Л.Р. Ахметзяновой.

Тема исследований диссертации является практически значимой – область применения AEAD-систем обширна, - и актуальной – известно не очень много научных работ, посвященных этим вопросам, и, кроме того, разнообразие типов AEAD-режимов требует отдельного изучения каждого из них с учетом индивидуальных особенностей. Получение строго обоснованных нижних оценок уровня стойкости криптографических схем в целевых математических моделях нарушителя в зависимости от уровня стойкости базового БСА, параметров схемы и ограничений на ресурсы нарушителя позволяет минимизировать количество «точек доверия», для которых нет возможности получить оценки стойкости, и тем самым повысить надежность выводов о стойкости схемы.

В диссертации Л.Р. Ахметзяновой представлены решения следующих задач:
1) разработка методов получения верхних и нижних оценок уровня стойкости в базовых моделях нарушителя для некоторых AEAD-режимов, которые рассматривались в качестве стандартов Российской Федерации;
2) разработка нового AEAD-режима с целью достижения стойкости в расширенных моделях нарушителя, учитывающих возможность повторного использования некоторых начальных параметров (вектора инициализации);
3) разработка методов стойкого улучшения существующих AEAD-режимов с целью увеличения объема безопасно обрабатываемых данных.

Диссертация Л.Р. Ахметзяновой состоит из шести разделов и приложения. В первом разделе (Введение) описаны принципы устройства AEAD-схем, приведен очень краткий обзор наиболее известных AEAD-схем, описаны особенности их использования, основные задачи криптографического анализа и принципиальные трудности их решения. Здесь же сформулированы цели диссертации, обоснована актуальность темы исследования, ее теоретическая и практическая значимость, сформулированы основные результаты диссертации и отмечены главные черты, составляющие их новизну. В этом разделе также перечислены публикации автора по теме диссертации и дано краткое описание ее содержания. Значительная часть материала этого раздела содержится в автореферате диссертации.

Во втором разделе (Обозначения, определения и общие сведения) описаны обозначения, используемые далее во всех разделах диссертации, введена согласованная система терминов и понятий, необходимых для построения математических моделей противника (нарушителя), применительно к AEAD-схемам. В следующем разделе (Свойства безопасности AEAD-схем) приведены определения рассматриваемых в диссертации целевых функций угрозы (преобладания нарушителя) в различных моделях. Здесь же показано, что оценка стойкости AEAD-схем может быть составлена из двух независимых оценок: 1) стойкости AEAD-режимов в модели со случайной подстановкой, и 2) стойкости БСА, используемого в AEAD-схеме. Именно этот известный результат дает основание для проведения самостоятельного независимого изучения оценок стойкости AEAD-режимов при помощи чисто комбинаторных методов.

Можно отметить, что вводные разделы диссертации написаны очень хорошим научным стилем, свод определений вполне систематизирован, основные задачи исследования четко сформулированы, их научная и практическая значимость обоснованы.

В последующих разделах диссертации представлены решения трех основных задач этой научной работы. В первом из них (Глава 1) проведен анализ уровня стойкости двух ранее известных AEAD-режимов, имеющих названия «8 бит» и MGM (Multilinear Galois Mode). Для режима «8 бит» автором предложен метод нарушения свойства целостности, который демонстрирует, что предложенный режим обладает заведомо не лучшими свойствами в сравнении с другими претендентами, но при этом уступает им по производительности. Этот метод явно описан в виде последовательности шагов взаимодействия противника с AEAD-схемой и оценкой вероятности, с которой ему оказывается возможным сформировать корректные коды аутентификации для некоторого числа новых

сообщений (Теорема 1.1.1). Для режима MGM автором получена нижняя оценка уровня стойкости в базовой модели нарушителя IND-CPA, которая показывает, что режим обеспечивает достаточный уровень стойкости в части конфиденциальности. Решающая роль в получении этого результата отводится Лемме 1.2.1, в которой установлена верхняя оценка вероятности возникновения коллизии среди наборов, поступающих на вход функции инициализации. Эта комбинаторная лемма имеет очень изощренное доказательство, и ее значение не ограничивается лишь результатами диссертации: с ее помощью другими исследователями удалось получить оценку уровня стойкости для свойства целостности режима MGM.

Во второй главе решена задача улучшения свойств режима MGM. Одним из ограничений применения этого режима является требование бесповторности векторов инициализации, которое далеко не всегда можно соблюсти на практике. Для преодоления этого недостатка автором диссертации была разработана модификация режима MGM, названная MGM2. Основное различие между двумя режимами заключается в способе создания секретных маскирующих блоков и секретных коэффициентов мультилинейной функции. Введенные модификации, не ухудшающие производительность оригинального режима, позволили доказать улучшенные оценки стойкости даже в расширенных моделях, в которых у нарушителя появляется дополнительная возможность навязывать одинаковые значения вектора инициализации для обработки сообщений. Центральными результатами этой главы являются Теорема 2.1.1 (оценка уровня стойкости MGM2-схемы для свойства целостности) и Теорема 2.1.2. (оценка уровня стойкости MGM2-схемы для свойства конфиденциальности). Эти оценки были получены в моделях нарушителя, учитывающих возможность повтора векторов инициализации. Особенно важным, по мнению рецензента, является то обстоятельство, что изменения, внесенные в исходный MGM-режим, формировались фактически по ходу получения упомянутых оценок.

Третья глава содержит результаты исследований по улучшению комбинаторных свойств повсеместно используемых режимов OMAC и GCM с целью продления сроков использования секретных ключей. Это может быть достигнуто при помощи метода внутреннего преобразования секрета (re-keying), предложенного С.В. Смышляевым. Именно этот метод был применен для модификации известных ранее режимов OMAC и GCM. Заслугой автора диссертации здесь является развитие метода внутреннего преобразования

секрета для обеспечения целостности и соответствующих методов обоснования оценок уровня безопасности, которые ранее были применимы только для исследования конфиденциальности. На основе режима вычисления кодов аутентификации OMAC был разработан новый комбинированный режим OMAC-ACPKM-Master, для которого доказана нижняя оценка стойкости в модели с использованием псевдослучайных функций (теорема 3.1.1 и сопутствующий ей ряд комбинаторных лемм). На основе AEAD-режима GCM был разработан режим GCM-ACPKM, для которого доказана нижняя оценка стойкости в отношении свойства целостности (теорема 3.2.2). Доказанные оценки демонстрируют, что разработанные режимы обладают лучшими комбинаторными свойствами в сравнении с оригиналами, что позволяет безопасно обрабатывать значительно больший объем данных без существенного ухудшения производительности.

Таким образом, диссертация Л.Р. Ахметзяновой представляет собой завершенное научное исследование трудных математических задач получения и обоснования нижних оценок стойкости по отношению к свойствам конфиденциальности и целостности для целой серии криптографических алгоритмов аутентифицированного шифрования с ассоциированными данными. При решении этих задач автору пришлось проявить немало изобретательности и искусного владения комбинаторной техникой для получения как можно более точных оценок вероятности событий, свидетельствующих о нарушении требований безопасности анализируемых криптографических схем. Математические обоснования всех утверждений работы проведены корректно и подробно. Помимо собственно математических результатов к достижениям работы можно отнести также творческое обращение с комбинаторными методами, которые используются автором как средства направленного поиска улучшений и модификаций известных криптографических алгоритмов. Все результаты, полученные в диссертации, имеют корректные формулировки и обоснованы строгими доказательствами. Результаты работы изложены в 5 публикациях в изданиях, индексируемых в Web of Science, Scopus, RSCI и из списка ВАК Минобрнауки России; из них 3 — в изданиях, индексируемых в Web of Science, Scopus, RSCI, а также представлены на нескольких международных конференциях и научных семинарах.

Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность» по областям исследований, указанным в пп. 1, 4, 9 и 13 Паспорта специальности.

Необходимо отметить и некоторые недостатки диссертации.

1). Работа выдержана в строгом и лаконичном научном стиле, который не вызывает сколь-нибудь серьезных замечаний. Однако в работе все же встречаются некоторые, к чести автора, немногочисленные изъяны. В определении 0.1 (стр. 29) интерактивного алгоритма принцип взаимодействия агентов лишь подразумевается, но не определен в явном виде. В комментарии к определению 0.2 (стр. 35) говорится о «нарушении целостности принятых сообщений», хотя ни о каких сообщениях в этом определении не упоминается. На стр. 42 используется крайне неудачное выражение «параметризованное параметром». На стр. 49 используется операция <<, которая не была определена нигде ранее в тексте. Функция инициализации, играющая главную роль в лемме 1.2.1, обозначена на стр. 61 безликим символом f, редко упоминаемым далее и вызывающим трудности в понимании смысла обозначения D^i на стр. 66.

2) Автор диссертации уделил очень мало внимания обзору известных ранее работ, посвященных анализу стойкости AEAD-схем, и сравнительному анализу используемых в этих работах методах получения оценок стойкости. В частности, в списке литературы не упомянута важная статья M. Bellare, P. Rogaway, D. Wagner. The EAX Mode of Operation (A Two-Pass Authenticated Encryption Scheme Optimized for Simplicity and Efficiency). Fast Software Encryption (FSE) 2004, в которой также были решены задачи получения оценок стойкости для одной AEAD-схемы, и не проведено сопоставление методов, используемых в этой статье, и тех методов, которые были разработаны и развиты в диссертации. Это замечание имеет непосредственное отношение к вопросу о новизне полученных результатов. Нет ни малейших сомнений, что все математические результаты, представленные в диссертации, являются новыми. Но обсуждение степени их методической новизны в диссертации совершенно отсутствует.

3) В заключении диссертации автор избегает обсуждения перспектив дальнейшего развития и применения предложенных методов анализа стойкости для других AEAD-режимов; это обсуждение ограничилось лишь общими словами. Вместе с тем, для понимания значимости полученных результатов важно проанализировать, насколько универсальными являются и сам подход к оценке уровня стойкости AEAD-схем и те комбинаторные методы, которые были предложены автором диссертации для реализации этого подхода.

Эти замечания относятся исключительно к форме представления результатов диссертации, но не их математическому качеству, которое, по мнению рецензента, является очень высоким.

Заключительная оценка.

Диссертация Ахметзяновой Лилии Руслановны соответствует паспорту научной специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Она отвечает требованиям, предъявляемым к кандидатским диссертациям Московским государственным университетом имени М.В. Ломоносова, в частности, требованиям пп. 2.1 – 2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова, и оформлена в соответствии с приложениями 5 и 6 Положения о диссертационном совете Московского государственного университета имени М.В. Ломоносова.

Считаю, что соискатель Ахметзянова Лилия Руслановна безусловно заслуживает присуждения ей ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Официальный оппонент,

профессор кафедры математической кибернетики

факультета ВМК МГУ им. М.В. Ломоносова,

д.ф.-м.н. [redacted] В. А. Захаров

Контактная информация:

адрес: 119991, Москва, ГСП-1, Ленинские горы,
МГУ имени М.В. Ломоносова, 2-й учебный корпус.
e-mail: zakh@cs.msu.ru,

тел. +7 (495) 939-53-92.

Подпись В. А. Захарова удостоверяю

Декан факультета ВМК

МГУ имени М.В. Ломоносова,

академик РАН И.А. Соколов