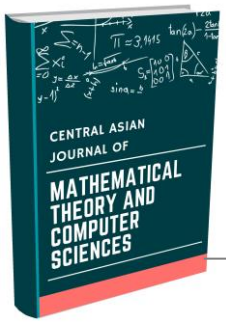

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

http://cajmtcs.centralasianstudies.org/index.php/CAJMTCS

Volume: 02 Issue: 11 | Nov 2021 ISSN: 2660-5309

Исследование особенностей критерия стойкости алгоритма хеш-функции

Д. Е. Акбаров[1], О. Э.Кушматов[2], Ш.А. Умаров[3], А. К. Шаев ст [4]

[1]д.физ.-мат. н., Какандский государственный педагогический институт, Каканд, Узбекистан

[2]к.физ.-мат. н., Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан

[3]исследователь, Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан

[4]Преподаватель, Ферганский политехнический институт, Фергана, Узбекистан

Аннотатсия:

В статье исследованы особенности критериев стойкости алгоритма хеш-функции. Выявлены общие свойства моделей хеш-функции. На их основе сформулированы соответствующие требования в виде критериев, определяющие необходимые условия криптографической стойкости. Эти критерии сформулированы как утверждение. Описаны назначения хеш-функции при решении задач информационной безопасности. Рассмотрены особенности конструкции алгоритма хеш-функции с обоснованиями криптографических свойств.

ARTICLEINFO

Article history:
Received 30 Sep 2021
Revised form 22 Oct 2021
Accepted 17 Nov 2021

Ключевые слова: алгоритм хеш-функции, необходимое условие, математическая модель, преобразование распространения, преобразование перемешивания, коллизия, хешируемое сообщение, нелинейность, односторонность, лавинный эффект, гибкость относительно корреляции, конструкция алгоритма, без ключевые хеш-функции, ключевые хеш-функции.

----------***----------

Введение. Хеш-функцией называется преобразование сжатия сообщения любой ограниченной длины в битах или байтах на фиксированной относительно малой длины блока сообщения.

Основные назначения хеш-функции, следующие:

1) При проведении статистических исследований над сообщениями большого объема и сохранении хеш-значения для проверки целостности сообщения;

2) При тестовой проверке правильного функционирования логических и вычислительных средств с сравнением большого объема входных данных соответствующими фиксированной малой длины выходными данными;

3) При разработке алгоритма быстрого нахождения электронных сообщений большого объема;

4) В алгоритмах электронной цифровой подписи для идентификации автора сообщения и проверки действительности;

5) При проверке целостности, т.е. проверки без изменения базы электронных данных и других многих задач информационных технологий.

О хеш-функциях более подробное научные и практическое сведения можно получить из литературных источников [1-7] и др.

Постановка задачи. В предлагаемой статье исследованы вопросы необходимого условия криптографической стойкости хеш-функции. Так как интенсивное развитие теории и их приложения, вычислительной техники и технологии требует постоянного дополнения к требованиям криптографической стойкости алгоритмов.

Решение задачи. Свойство односторонности, логические операции, талблица сжатия, логические функции, операция $\oplus -$ XOR, выполнение операции с неизвестным значением параметра и другие такие операции обеспечивают криптографическую стойкость преобразования алгоритмов хэш-функции. Следующее утверждение, сформулированное как необходимое условие криптографической стойкости алгоритма хеш-функции, основано на системном изучении и исследованиях в этой области науки [8-13].

Утверждение. *Если алгоритм хеш-функции криптографически стойкий, то должно выполняться следующие условия:*

1) Открытость а*лгоритма хэш-функции, его криптостойкость зависит от особенностей преобразования, в случае хэш-функции с ключом зависит еще от секретного хранения и длины ключа. Задаётся длина ключа не меньше 256 символов в битах;*
2) *Должен быть применимым любому сообщению x ограниченной длиной;*
3) *Результат хеширования – значение хэш-функции должно быть фиксированной длины $(256+32\times l),\ \ l=0,1,2,\ldots<\infty$, т. е. не меньше 256 в битах;*
4) *По произвольному x вычисление значение $h(x)=H$ хэш-функции должна быть легко вычислима;*
5) *По данному значению H хэш-функции, нахождение такого x, которое удовлетворяет равенству $h(x)=H$, сложно разрешима – практически экономически невыгодная задача.*
6) *Для $\forall x$ и $\forall y\neq x$ обеспечено неравенство $h(x)\neq h(y)$ (стойкость относительно коллизии) ;*
7) *Длина преобразуемых не меньше 256 в битах $k=k_1k_2...k_N,\ \ k_i\in\{0;1\}, N=32\times l,\ \ l=4,5,\ldots<\infty$ и операции, применяемые в преобразованиях алгоритма, соответствуют удобному использованию в микропроцессорах, микроконтроллерах и компьютерных вычислительных устройствах;*
8) *Основные базовые преобразования должны обладать свойством эффективного перемешивания и распространения, которые обеспечатся особенностями: односторонности, равновесия, регулярности, лавинного эффекта, гибкости относительно корреляции и т.д.;*
9) *Основные базовые преобразования, при известном промежуточном результате, обладают свойством односторонности.*

Доказательство. Так как предложенное утверждение выражает необходимое условие крипкостойкости, то для проверки этих условий в конкретных предложенных алгоритмах хеш функции требуется проверить следующие свойства в его базовых преобразованиях: односторонности, равновесия, регулярности, лавинного эффекта, гибкости относительно корреляции и т.д. Эти свойства в совокупности выражает эффективное распространение и рассеивания битов сообщения.

Критерий 1) обеспечивает, чтобы не было сомнения в криптогрфической стойкости алгоритма хеш-функции. Кроме того, означает, что соблюден принцип Кирхгофса. Неизвестность алгоритма хеш-функции часто порождает недоверие криптографической стойкости.

Проверка этого условия осуществляется непосредственным и открыто объявлением алгоритма и его криптографических свойств.

Критерий 2) обеспечивает широкие возможности использования алгоритма в практических приложениях.

Критерий 3) будет основой обспечения криптографической стойкости алгоритма хэш-функции к разным криптоатакам. То есть, если длина значения хеш-функции не меньше $(256+32\times l)$ *бит,* $l=0,1,2,\ldots<\infty$, то фабрикация сообщение по заданному значению хеш-функции усложняется.

Критерий 4) позволят достаточно быстро вычислить значение хеш-функции большого объема сообщения.

Целью, улучшения криптографической стойкости, использования преобразований, требующих сложных вычислений в алгоритме хеш-функции, часто приводит неэффективному практическому приложению.

Это условие проверяется электронно-вычислительными средствами. Проверяются основы моделей базовых преобразований. Если в совокупности базовых преобразований имеются: логические операции, табличные замены, логической функции и другие, легко вычисляемые модели со свойствами эффективного распространения и перемешивания, то они являются криптографически значимыми. Криптографическая эффективность преобразования распространения и перемешивания проверяется сравнением попарно разным входам постановкой в соответствие попарно разные выходы или наоборот [11-14].

Критерий 5) означает выполнение требования односторонности преобразования алгоритма хеш-функции. Если по известному значению H хеш-функции вычисление соответствующего текста x относительно несложно $h(x)=H$, то это обстоятельство является основой для фабрикации – коллизии. Этот критерий проверяется определением не существования обратных преобразований относительно базовых.

Критерий 6) означает требование сложности нахождения пары сообщений x и $y\neq x$, имеющие одинаковые значения хеш-функции, т.е. является условием стойкости в коллизии.

Проверка этого критерия осуществляется следующим образом. По алгоритму хеш-функции проверяется условия попарно разным входным блокам $x_i=\left(x_1^i x_2^i \ldots x_{256}^i\right)$, $x_j^i\in\{0;1\}$, $j=1,\ldots,256;$ $i=0,1,\ldots,2^{256}-1$; сопоставлены попарно разные $y_i=\left(y_1^i y_2^i \ldots y_{256}^i\right)$ $y_j^i\in\{0;1\}$, $j=1,\ldots,256;$ $i=0,1,\ldots,2^{256}-1$, значения хеш-функции. Необходимость критерия 6 заключается в том, что длина значения хеш-функции не менее 256 битов обеспечит неэффективность проверки всех попарно разных возможных входов.

Критерий 7) ограничивает возможности криптографической атаки полного выбора возможных блоков проверки и соответствующих выходов. Означает требования при необходимости эффективного модифицирования алгоритма с сохранением основ базовых преобразования и их аппаратной реализации при решении соответствующих прикладных задач.

Критерий 8) необходим для обеспечения стойкости преобразования алгоритма к криптографическим атакам разного типа.

Свойства эффективного рассеивания и распространения основных базовых преобразований, нелинйность, равновесие, регулярность, лавинный эффект, корреляционная иммунность и другие соответствующие особенности вместе обеспечат надёжную стойкость алгоритма. Не оставляет место для возможных криптографических атак.

Критерий 9) обеспечит требование невозможности обратного преобразования при некотором известном промежуточном результате.

Таким образом, процесс хеширования является алгоритмом сжатия пробразования, удовлетворяющий требованиям предложенного утверждения. Эти алгоритмы могут быть без ключевым или ключевым.

Специалистами признано, что стандарты алгоритма хеш-функции должны быть без ключа. Это по существу, так как алгоритм без ключа и его открытость ограничивает недоверие среди пользователей информационно-коммуникационной сети. Кроме того, в конец хешируемого текста в виде конкатенации присоединяются следующие:

1) **Присоединение битов дополнения** – если длина последнего блока меньше 256 бита, то он дополнятся до 256 битов с символом пробела. Полученный таким образом текст называется расширенным текстом.
2) **Присоединение длины сообщения** – определяющая в битах длины сообщения вместе с битами дополнения, вычисленное значение по mod 2^{256} присоединяется в виде 256 битном блоке.
3) **Присоединение контрольной суммы** – на результат 2-этапа присоединяется 256 битный блок, означающий контрольную сумму сообщения. Блок, означающий контрольную сумму, определяется значением количества блоков расширенного текста, вычисленным по mod 2^{256} и присоединяется в виде 256 битный блок. Эти присоединенные дополнительные блоки увеличит стойкости алгоритма хеш-функции в коллизии.

Существующие виды криптографических атак на хеш-функции:

1. Криптографическая атака по преобразованиям хеш-функции;

2. Дифференциальный криптографический анализ по преобразованиям алгоритма хеш-функции;

3. Криптографическая атака на основе метода встречи текстов;

4. Криптографическая атака при известной длине и алфавите хешируемого сообщения, по выбору всех возможных 2^{256} входных цифровых блоков при длине 256 битных блоков хеш-значений и т. д.

Осуществление этих методов криптографических атак требуют разработки определённых соответствующих алгоритмов и приложений.

Заключение. В статье сформулированы и описаны сущности необходимых критериев, обеспечивающие стойкость хеш-функции. В общем виде обоснованы необходимые криптографические свойства базовых преобразований. Конкретные приложения и проверки критериев зависит от явного и конкретного вида моделей преобразований определенного алгоритма соответственно. Теоретическая и практическая ценность статьи заключается в систематизированной и более полной формулировке, а также выявления сущностей необходимых условий стойкости хеш-функций.

Отметим, что криптографический анализ преобразования хеш-функции по критериям в соответствии развитием вычислительной науки, требует периодических дополнений.

ИСПОЛЬЗОВАННЫЕ ЛИТЕРАТУРЫ

1. Шнайер, Б. (2002). Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. *М.: Триумф*, *816*, 3.
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. (2002). Основы криптографии: Учебное пособие, 2-е изд. –М. Гелиос АРВ,. С. 480.
3. Харин, Ю. С., Берник, В. И., Матвеев, Г. В., & Агиевич, С. В. (2003). Математические и компьютерные основы криптологии.
4. Ростовцев, А. Г., & Маховенко, Е. Б. (2005). Теоретическая криптография. *СПб.: АНО НПО «Профессионал*.
5. Молдовян А. А., Молдовян Н. А., Советов Б. Я.. (2001). Криптография. – Санкт-Петербург, Изд. «Лань»,.с. 224.
6. Akbarov D. E. (2009). Cryptographic methods of ensuring information security and their application. Tashkent. p. 432.
7. Акбаров, Д. Е., Умаров, Ш. А., & Акбаров, Д. Є. (2016). Алгоритм хеш-функции с новыми базовыми преобразованиями.
8. Hayotov, A. R., Bozarov, B. I., & Abduganiev, A. (2018). Optimal formula for numerical integration on two dimensional sphere. *Uzbek Mathematical Journal*, *3*, 80-89.
9. Bozarov, B. I. (2019). An optimal quadrature formula with sinx weight function in the Sobolev space. *Uzbekistan academy of sciences vi romanovskiy institute of mathematics*, 47.
10. Hayotov, A., & Bozarov, B. (2021, July). Optimal quadrature formulas with the trigonometric weight in the Sobolev space. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020022). AIP Publishing LLC.
11. Каримов, Ш. Т., & Хожиакбарова, Г. (2017). Аналог задачи гурса для одного неклассического уравнения третьего порядка с сингулярным коэффициентом. *Toshkent shahridagi turin politexnika universiteti*, 121.
12. Tillabayev, B., & Bahodirov, N. (2021). Solving the boundary problem by the method of green's function for the simple differential equation of the second order linear. *ACADEMICIA: An International Multidisciplinary Research Journal*, *11*(6), 301-304.
13. Kosimov, H., & Tillabaev, B. (2018). Mixed fractional order integral and derivatives for functions of many variables. *Scientific journal of the Fergana State University*, *1*(2), 5-11.
14. Ахмедова, Г. А., & Файзуллаев, Ж. И. (2014). Управление инновационной активностью промышленных предприятий на основе эффективных методов ее оценки и стимулирования. *Актуальные проблемы гуманитарных и естественных наук*, (4-1).