



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК

G06F 11/08 (2020.02); G06F 21/64 (2020.02)

(21)(22) Заявка: 2019143386, 19.12.2019

(24) Дата начала отсчета срока действия патента:
19.12.2019

Дата регистрации:
21.08.2020

Приоритет(ы):

(22) Дата подачи заявки: 19.12.2019

(45) Опубликовано: 21.08.2020 Бюл. № 24

Адрес для переписки:

350063, г. Краснодар, ул. Красина, 4,
Краснодарское высшее военное училище,
Комиссаровой Т.П.

(72) Автор(ы):

Диченко Сергей Александрович (RU),
Самойленко Дмитрий Владимирович (RU),
Финько Олег Анатольевич (RU)

(73) Патентообладатель(и):

федеральное государственное казенное
военное образовательное учреждение
высшего образования "Краснодарское
высшее военное орденов Жукова и
Октябрьской Революции Краснознаменное
училище имени генерала армии С.М.
Штеменко" (RU)

(56) Список документов, цитированных в отчете
о поиске: RU 2680033 C2, 14.02.2019. RU
2696425 C1, 02.08.2019. US 2003/0126400 A1,
03.07.2003. US 2005/0235154 A1, 20.10.2005.

(54) СПОСОБ КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ НА ОСНОВЕ КРИПТОГРАФИЧЕСКОГО ТРЕУГОЛЬНИКА ПАСКАЛЯ

(57) Реферат:

Изобретение относится к области вычислительной техники. Техническим результатом является обеспечение контроля целостности данных на основе криптографического треугольника Паскаля. Раскрыт способ контроля целостности данных на основе криптографического треугольника Паскаля, заключающийся в том, что обнаружение и локализация возникающей ошибки в подблоках $m_1, m_2, \dots, m_k$ блока данных M обеспечиваются посредством вычисления системы хэш-кодов, формируемой из хэш-кодов хэш-функции от совокупности подблоков данных, и ее сравнения с эталонной, при этом блок данных M для осуществления контроля целостности представляется в виде подблоков фиксированной длины $m_1, m_2, \dots, m_k$, к которым применяется хэш-функция по правилам построения треугольника Паскаля, где схема хэширования содержит

таблицу, имеющую треугольную форму, в которой по бокам размещены подблоки $m_1, m_2, \dots, m_k$ блока данных M , подлежащие защите, внутри треугольника - промежуточные результаты преобразований:

$$s_1^{(1)} = h(m_1, m_2), \dots,$$

$$s_1^{(t/2)} = h(m_{t-1}, s_1^{(t/2-1)}), \dots, \text{внизу - значения}$$

хэш-кодов $s_z^{(k/2)}$, где $z = 1, 2, \dots, k/2$, которые вычисляются от подблоков m_{k-1} и m_k блока данных M , подлежащих защите, и нижних результатов промежуточных преобразований:

$$s_1^{(k/2-1)}, \dots, s_{k/2-1}^{(k/2-1)}; s_1^{(0)} \text{ и } s_2^{(0)} \text{ вычисляются по}$$

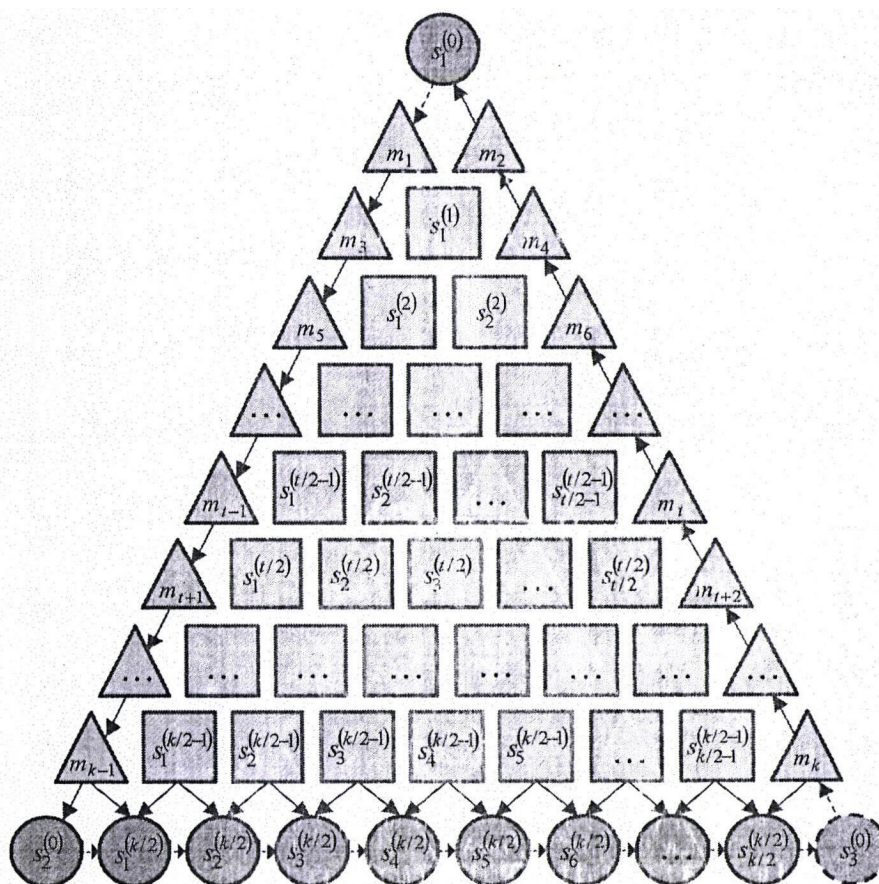
$$\text{формулам: } s_1^{(0)} = h(m_2, \dots, m_t, \dots, m_k, s_3^{(0)})$$

$$\text{и } s_2^{(0)} = h(m_1, \dots, m_{t-1}, \dots, m_{k-1}, s_1^{(0)})$$

соответственно, при этом контроль целостности

подблоков $m_1, m_2, \dots, m_k$ блока данных M осуществляется путем сравнения значений вычисленных при запросе на использование защищаемых данных хэш-кодов со значениями

эталонных хэш-кодов $s_z^{(k/2)}, s_1^{(0)}, s_2^{(0)}$, вычисленных ранее, для контроля целостности которых вычисляется хэш-код $s_3^{(0)}$. 6 ил.



Общая схема применения хэш-функции, основанная на правилах построения треугольника Паскаля

Фиг. 2



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) ABSTRACT OF INVENTION

(52) CPC

G06F 11/08 (2020.02); G06F 21/64 (2020.02)

(21)(22) Application: 2019143386, 19.12.2019

(24) Effective date for property rights:
19.12.2019Registration date:
21.08.2020

Priority:

(22) Date of filing: 19.12.2019

(45) Date of publication: 21.08.2020 Bull. № 24

Mail address:

350063, g. Krasnodar, ul. Krasina, 4, Krasnodarskoe
vysshee voennoe uchilishche, Komissarovoj T.P.

(72) Inventor(s):

Dichenko Sergej Aleksandrovich (RU),
Samojlenko Dmitrij Vladimirovich (RU),
Finko Oleg Anatolevich (RU)

(73) Proprietor(s):

federalnoe gosudarstvennoe kazennoe voennoe
obrazovatelnoe uchrezhdenie vysshego
obrazovaniya "Krasnodarskoe vysshee voennoe
ordenov Zhukova i Oktyabrskoj Revolyutsii
Krasnoznamennoe uchilishche imeni generala
armii S.M. Shtemenko" (RU)

(54) DATA INTEGRITY CONTROL METHOD BASED ON PASCAL CRYPTOGRAPHIC TRIANGLE

(57) Abstract:

FIELD: computer equipment.

SUBSTANCE: invention relates to computer engineering. Disclosed is a method of controlling data integrity based on a Pascal cryptographic triangle, consisting in that detection and localization of occurring error in sub-blocks $m_1, m_2, \dots, m_k$ of data unit M are provided by calculating a hash code system formed from hash codes of the hash function from a plurality of data subblocks and comparing said reference data with a reference, wherein data unit M for integrity monitoring is presented in the form of sub-blocks of fixed length $m_1, m_2, \dots, m_k$, to which a hash function is used according to Pascal triangle construction rules, where the hashing scheme comprises a table having a triangular shape, in which there are sub-blocks $m_1, m_2, \dots, m_k$ on the sides of data unit M to be protected, inside the triangle – intermediate results of transformations:

$$s_1^{(1)} = h(m_1, m_2), \dots,$$

$$s_1^{(t/2)} = h(m_{t-1}, s_1^{(t/2-1)}), \dots, \text{lower – hash codes}$$

values $s_z^{(k/2)}$, where $z = 1, 2, \dots, k/2$, which are calculated from subblocks m_{k-1} and m_k of data unit M to be protected, and lower results of intermediate transformations: $s_1^{(k/2-1)}, \dots, s_{k/2-1}^{(k/2-1)}$; $s_1^{(0)}$ and $s_2^{(0)}$ are calculated using the formulas:

$$s_1^{(0)} = h(m_2, \dots, m_t, \dots, m_k, s_3^{(0)}) \quad \text{and}$$

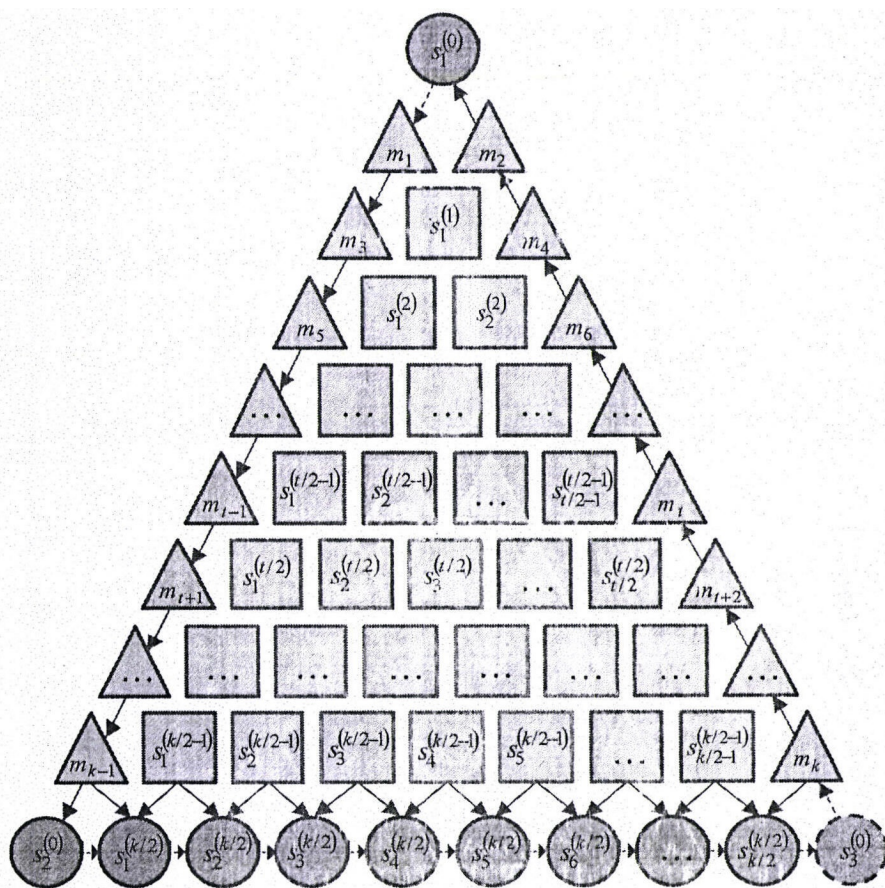
$$s_2^{(t)} = h(m_1, \dots, m_{t-1}, \dots, m_{k-1}, s_1^{(0)})$$
 respectively, wherein control of integrity of sub-blocks $m_1, m_2, \dots, m_k$ of data unit M is performed by comparing values of hash codes calculated with request for use of protected data with values of reference hash codes $s_z^{(k/2)}, s_1^{(0)}, s_2^{(0)}$, previously calculated, to control the integrity of which is calculated hash code $s_3^{(0)}$.

EFFECT: control of data integrity based on the Pascal cryptographic triangle.

1 cl, 6 dwg

RU 2 730 365 C1

RU 2 730 365 C1



Общая схема применения хэш-функции, основанная
на правилах построения треугольника Паскаля

Фиг. 2

Область техники, к которой относится изобретение

Предлагаемое изобретение относится к информационным технологиям и может быть использовано для контроля целостности информации в системах хранения данных на основе применения криптографических хэш-функций к защищаемым блокам данных в условиях деструктивных воздействий злоумышленника и среды.

Уровень техники

а) Описание аналогов

Известны способы контроля целостности данных за счет применения криптографических методов: ключевое и бесключевое хэширование, средства электронной подписи (Патент на изобретение RUS №2680033 22.05.2017; Патент на изобретение RUS №2680739 28.11.2017; Патент на изобретение RUS №2696425 22.05.2018: Кнут, Д.Э. Искусство программирования для ЭВМ. Том 3 сортировка и поиск [Текст] / Д.Э. Кнут. - М.: «Мир», 1978. - 824 с.; Dichenko, S. Two-dimensional control and assurance of data integrity in information systems based on residue number system codes and cryptographic hash functions / S. Dichenko, O. Finko // Integrating Research Agendas and Devising Joint Challenges International Multidisciplinary Symposium ICT Research in Russian Federation and Europe. 2018. P. 139-146; Samoylenko, D. Protection of information from imitation on the basis of crypt-code structures / D. Samoylenko, M. Ereemeev, O. Finko, S. Dichenko // Advances in Intelligent Systems and Computing. 2019. №889. P. 317-331; Диченко, С.А. Контроль и обеспечение целостности информации в системах хранения данных. Научные технологии в космических исследованиях Земли. - 2019. - Т. 11. - №1. - С. 49-57; Диченко, С.А. Гибридный крипто-кодовый метод контроля и восстановления целостности данных для защищенных информационно-аналитических систем / С. Диченко, О. Финько // Вопросы кибербезопасности. - 2019. - №6(34). - С. 17-36), для которых типичны две обобщенные схемы получения хэш-кодов: для каждого подблока в блоке данных и для

целого блока данных.

Недостатками данных способов являются:

- высокая избыточность при контроле целостности последовательности подблоков блока данных небольшой размерности (при хэшировании каждого подблока в блоке данных);

- отсутствие возможности локализации искаженных подблоков в блоке данных (при хэшировании целого блока данных);

- отсутствие возможности осуществления контроля целостности эталонных хэш-кодов, предназначенных для осуществления контроля целостности защищаемых данных.

б) Описание ближайшего аналога (прототипа)

Наиболее близким по технической сущности к заявленному изобретению (прототипом) является способ обеспечения целостности данных в автоматизированных системах на основе линейных систем хэш-кодов, полученных с помощью стандартной процедуры реализации хэш-функции от совокупности данных в порядке, определенном специальной процедурой выбора подблока, основанной на математическом аппарате линейной алгебры (линейных систем хэш-кодов) (Финько, О.А. Обеспечение целостности данных в автоматизированных системах на основе линейных систем хэш-кодов, О.А. Финько, С.В. Савин // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. - 2015. - №114. - С. 796-811), где контроль целостности данных (обнаружение ошибки) по аналогии с линейными кодами осуществляется за счет вычисления синдрома, при проверке которого можно сделать вывод о нарушении целостности данных (наличии ошибки) (фиг. 1).

Недостатком известного способа является отсутствие возможности осуществления

контроля целостности эталонных хэш-кодов в условиях деструктивных воздействий злоумышленника и среды.

Раскрытие изобретения

а) Технический результат, на достижение которого направлено изобретение

5 Целью настоящего изобретения является разработка способа контроля целостности данных на основе применения криптографических хэш-функций к защищаемым блокам данных с возможностью осуществления контроля целостности эталонных хэш-кодов в условиях деструктивных воздействий злоумышленника и среды.

б) Совокупность существенных признаков

10 Поставленная цель достигается тем, что в известном способе обеспечения целостности данных, заключающемся в том, что обнаружение и локализация возникающей ошибки в подблоках $m_1, m_2, \dots, m_k$ блока данных M обеспечиваются посредством вычисления системы хэш-кодов, формируемой из хэш-кодов хэш-функции от совокупности подблоков данных, и ее сравнении с эталонной, в представленном же способе блок
15 данных M для осуществления контроля целостности представляется в виде подблоков фиксированной длины $m_1, m_2, \dots, m_k$, к которым применяется хэш-функция по правилам построения треугольника Паскаля, где схема хэширования содержит таблицу, имеющую треугольную форму, в которой по бокам размещены подблоки $m_1, m_2, \dots, m_k$ блока
20 данных M , подлежащие защите, внутри треугольника - промежуточные результаты преобразований: $s_1^{(1)} = h(m_1, m_2), \dots, s_1^{(t/2)} = h(m_{t-1}, s_1^{(t/2-1)}), \dots$, внизу - значения хэш-кодов $s_z^{(k/2)}$, где $z = 1, 2, \dots, k/2$, которые вычисляются от подблоков m_{k-1} и m_k блока данных M , подлежащих защите, и нижних результатов промежуточных преобразований:
25 $s_1^{(k/2-1)}, \dots, s_{k/2-1}^{(k/2-1)}, s_1^{(0)}$ и $s_2^{(0)}$ вычисляются по формулам: $s_1^{(0)} = h(m_2, \dots, m_t, \dots, m_k, s_3^{(0)})$ и $s_2^{(0)} = h(m_1, \dots, m_{t-1}, \dots, m_{k-1}, s_1^{(0)})$ соответственно, при этом контроль целостности подблоков $m_1, m_2, \dots, m_k$ блока данных M осуществляется путем сравнения значений вычисленных при запросе на использование защищаемых данных хэш-кодов со
30 значениями эталонных хэш-кодов $s_z^{(k/2)}, s_1^{(0)}, s_2^{(0)}$, вычисленных ранее, для контроля целостности которых вычисляется хэш-код $s_3^{(0)}$.

Сопоставительный анализ заявленного решения с прототипов показывает, что предлагаемый способ отличается от известного тем, что поставленная цель достигается за счет представления блока данных M подблоками фиксированной длины $m_1, m_2, \dots,$
35 m_k , к которым хэш-функция применяется по правилам построения треугольника Паскаля (Гарднер, М. Неисчерпаемое очарование треугольника Паскаля // Математические новеллы. - М.: Мир, 1974. - 456 с.), что позволяет осуществить контроль целостности эталонных хэш-кодов в условиях деструктивных воздействий злоумышленника и среды.

40 Контроль целостности блока данных M будет осуществляться путем сравнения значений вычисленных при запросе на использование защищаемых данных и эталонных хэш-кодов, что позволит в момент времени t в условиях деструктивных воздействий злоумышленника и среды определить данные, целостность которых была нарушена. Новым является то, что в предлагаемом способе блок данных M представляется в виде
45 подблоков фиксированной длины $m_1, m_2, \dots, m_k$, к которым хэш-функция применяется по правилам построения треугольника Паскаля. Новым является то, что применение хэш-функции по правилам построения треугольника Паскаля позволяет осуществить контроль целостности эталонных хэш-кодов, в частности, для контроля $s_2^{(0)}$ и $s_z^{(k/2)}$

вычисляется хэш-код $s_3^{(0)}$: $s_3^{(0)} = h(s_2^{(0)}, s_z^{(k/2)})$, контроль целостности которого осуществляется за счет его включения в процесс вычисления хэш-кода

$s_1^{(0)}$: $s_1^{(0)} = h(m_2, m_4, \dots, m_k, s_3^{(0)})$, контроль целостности которого, в свою очередь,

5 осуществляется за счет его включения в процесс вычисления хэш-кода

$s_2^{(0)}$: $s_2^{(0)} = h(m_1, m_3, \dots, m_{k-1}, s_1^{(0)})$.

в) Причинно-следственная связь между признаками и техническим результатом, Благодаря новой совокупности существенных признаков и слое обе реализована возможность:

10 - обнаружения ошибки, возникающей в защищаемых данных, в условиях деструктивных воздействий злоумышленника и среды:

- локализации обнаруженной ошибки;

- контроля целостности эталонных хэш-кодов, предназначенных для осуществления контроля целостности защищаемых данных.

15 Доказательства соответствия заявленного изобретения условиям патентоспособности «новизна» и «изобретательский уровень»

Проведенный анализ уровня техники позволил установить, что аналоги, характеризующиеся совокупностью признаков, тождественных всем признакам заявленного технического решения, отсутствуют, что указывает на соответствие 20 заявленного способа условию патентоспособности «новизна».

Результаты поиска известных решений в данной и смежных областях техники с целью выявления признаков, совпадающих с отличительными от прототипа признаками заявленного объекта, показали, что они не следуют явным образом из уровня техники. Из уровня техники также не выявлена известность отличительных существенных 25 признаков, обуславливающих тот же технический результат, который достигнут в заявленном способе. Следовательно, заявленное изобретение соответствует условию патентоспособности «изобретательский уровень».

Краткое описание чертежей

Заявленный способ поясняется чертежами, на которых показано:

30 фиг. 1 - общая схема формирования линейной системы хэш-кодов;

фиг. 2 - общая схема применения хэш-функции, основанная на правилах построения треугольника Паскаля;

фиг. 3 - общий вид сети хэширования для схемы применения хэш-функции;

35 фиг. 4 - схема контроля целостности эталонных хэш-кодов;

фиг. 5 - схема применения хэш-функции, основанная на правилах построения треугольника Паскаля (при $k=10$);

фиг. 6 - сеть хэширования для схемы применения хэш-функции к блоку данных (при $k=10$).

Осуществление изобретения

40 Блок данных М, подлежащий защите, для осуществления контроля целостности содержащихся в нем данных представляется в виде подблоков фиксированной длины

$$M = \{m_1 || m_2 || \dots || m_k\}.$$

где «||» обозначает операцию конкатенации, k - количество подблоков в блоке данных М.

45 М. Схема применения хэш-функции к блоку данных (фиг. 2), содержит таблицу, имеющую треугольную форму.

В этом треугольнике по бокам размещены подблоки m_i ($i=1, 2, \dots, k$) блока данных

М, подлежащие защите, внутри треугольника - промежуточные результаты преобразований:

$$s_1^{(1)} = h(m_1, m_2), \dots, s_1^{(t/2)} = h(m_{t-1}, s_1^{(t/2-1)}), \dots,$$

5 внизу - значения хэш-кодов $s_z^{(k/2)}$ ($z = 1, 2, \dots, k/2$), которые вычисляются от подблоков m_{k-1} и m_k блока данных М, подлежащих защите, и нижних результатов промежуточных преобразований:

$$s_1^{(k/2-1)}, s_2^{(k/2-1)}, \dots, s_{k/2-1}^{(k/2-1)};$$

10 $s_1^{(0)}$ и $s_2^{(0)}$ вычисляются соответственно по формулам:

$$s_1^{(0)} = h(m_2, m_4, \dots, m_t, m_{t+2}, \dots, m_k, s_3^{(0)}),$$

$$s_2^{(0)} = h(m_1, m_3, \dots, m_{t-1}, m_{t+1}, \dots, m_{k-1}, s_1^{(0)}).$$

15 Контроль целостности подблоков m_i блока данных М осуществляется путем сравнения значений вычисленных при запросе на использование защищаемых данных хэш-кодов со значениями эталонных хэш-кодов $s_z^{(k/2)}, s_1^{(0)}, s_2^{(0)}$, вычисленных ранее.

20 Для контроля целостности эталонных хэш-кодов (фиг. 3). в частности, $s_2^{(0)}$ и $s_z^{(k/2)}$ вычисляется хэш-код $s_3^{(0)}$:

$$s_3^{(0)} = h(s_2^{(0)}, s_z^{(k/2)}).$$

25 контроль целостности которого, в свою очередь, осуществляется за счет его включения в процесс вычисления хэш-кода $s_1^{(0)}$:

$$s_1^{(0)} = h(m_2, m_4, \dots, m_k, s_3^{(0)}).$$

30 Контроль целостности хэш-кода $s_1^{(0)}$ осуществляется за счет его включения в процесс вычисления хэш-кода $s_2^{(0)}$:

$$s_2^{(0)} = h(m_1, m_3, \dots, m_{k-1}, s_1^{(0)}).$$

35 Данные хэш-коды будут являться эталонными для хэш-кодов, предназначенных для осуществления контроля целостности защищаемых данных (фиг. 4).

Пример

Рассмотрим схему применения хэш-функции (фиг. 5), основанную на правилах построения треугольника Паскаля для блока данных (при $k=10$)

40 Построим сеть хэширования (фиг. 6) для схемы применения хэш-функции к блоку данных (при $k=10$).

На основе сети хэширования получим синдромы вида

($s_3^{(0)}, s_2^{(0)}, s_1^{(0)}, s_5^{(5)}, s_4^{(5)}, s_3^{(5)}, s_2^{(5)}, s_1^{(5)}$) для локализации однократной ошибки, возникающей как в защищаемых данных, так и в контрольной информации:

45

$(0, 0, 0, 0, 0, 0, 0, 0) \rightarrow$ нет ошибки;

$(0, 0, 0, 1, 0, 0, 0, 0) \rightarrow [\tilde{m}_{11}];$

5 $(0, 0, 0, 0, 0, 0, 0, 1) \rightarrow [\tilde{m}_9];$

$(0, 0, 0, 1, 1, 0, 0, 0) \rightarrow [\tilde{m}_8];$

$(0, 0, 0, 0, 0, 0, 1, 1) \rightarrow [\tilde{m}_7];$

10 $(0, 0, 0, 1, 1, 1, 0, 0) \rightarrow [\tilde{m}_6];$

$(0, 0, 0, 0, 0, 1, 1, 1) \rightarrow [\tilde{m}_5];$

$(0, 0, 0, 1, 1, 1, 1, 0) \rightarrow [\tilde{m}_4];$

15 $(0, 0, 0, 0, 1, 1, 1, 1) \rightarrow [\tilde{m}_3];$

$(0, 0, 1, 1, 1, 1, 1, 1) \rightarrow [\tilde{m}_2];$

$(0, 1, 0, 1, 1, 1, 1, 1) \rightarrow [\tilde{m}_1];$

20 $(-, 1, -, 0, 0, 0, 0, 0) \rightarrow [\tilde{s}_1^{(0)}];$

$(-, -, 1, 0, 0, 0, 0, 0) \rightarrow [\tilde{s}_3^{(0)}];$

$(1, -, -, 0, 0, 0, 0, 0) \rightarrow [\tilde{s}_2^{(0)}] \text{ или } [\tilde{s}_5^{(5)}],$

25 где $[\tilde{\cdot}]$ - обозначает локализованный подблок $\tilde{m}_i$ блока данных М с нарушением целостности или хэш-коды $\tilde{s}_{z_j}^{(z_i)}$ ($z_i, z_j \in \{1, 2, \dots, 5\}$), $\tilde{s}_1^{(0)}$, $\tilde{s}_2^{(0)}$, $\tilde{s}_3^{(0)}$.

Таким образом, применение хэш-функции к защищаемым данным по правилам построения треугольника Паскаля позволяет осуществить контроль целостности, в том числе, эталонных хэш-кодов.

30

(57) Формула изобретения

Способ контроля целостности данных на основе криптографического треугольника Паскаля, заключающийся в том, что обнаружение и локализация возникающей ошибки в подблоках $m_1, m_2, \dots, m_k$ блока данных М обеспечиваются посредством вычисления

35 системы хэш-кодов, формируемой из хэш-кодов хэш-функции от совокупности подблоков данных, и ее сравнения с эталонной, отличающийся тем, что блок данных М для осуществления контроля целостности представляется в виде подблоков фиксированной длины $m_1, m_2, \dots, m_k$, к которым применяется хэш-функция по правилам

40 построения треугольника Паскаля, где схема хэширования содержит таблицу, имеющую треугольную форму, в которой по бокам размещены подблоки $m_1, m_2, \dots, m_k$ блока данных М, подлежащие защите, внутри треугольника - промежуточные результаты преобразований: $s_1^{(1)} = h(m_1, m_2), \dots, s_1^{(t/2)} = h(m_{t-1}, s_1^{(t/2-1)}), \dots$, внизу - значения хэш-кодов $s_z^{(k/2)}$, где $z = 1, 2, \dots, k/2$, которые вычисляются от подблоков m_{k-1} и m_k блока

45 данных М, подлежащих защите, и нижних результатов промежуточных преобразований: $s_1^{(k/2-1)}, \dots, s_{k/2-1}^{(k/2-1)}$; $s_1^{(0)}$ и $s_2^{(0)}$, вычисляются по формулам: $s_1^{(0)} = h(m_2, \dots, m_t, \dots, m_k, s_3^{(0)})$ и $s_2^{(0)} = h(m_1, \dots, m_{t-1}, \dots, m_{k-1}, s_1^{(0)})$ соответственно, при этом контроль целостности

подблоков $m_1, m_2, \dots, m_k$ блока данных M осуществляется путем сравнения значений
вычисленных при запросе на использование защищаемых данных хэш-кодов со
значениями эталонных хэш-кодов $s_z^{(k/2)}, s_1^{(0)}, s_2^{(0)}$, вычисленных ранее, для контроля
5 целостности которых вычисляется хэш-код $s_3^{(0)}$.

10

15

20

25

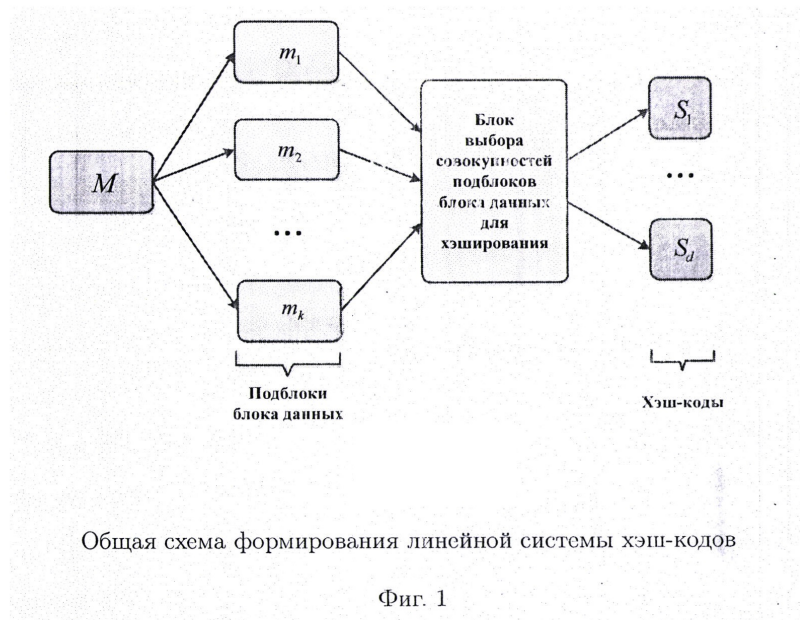
30

35

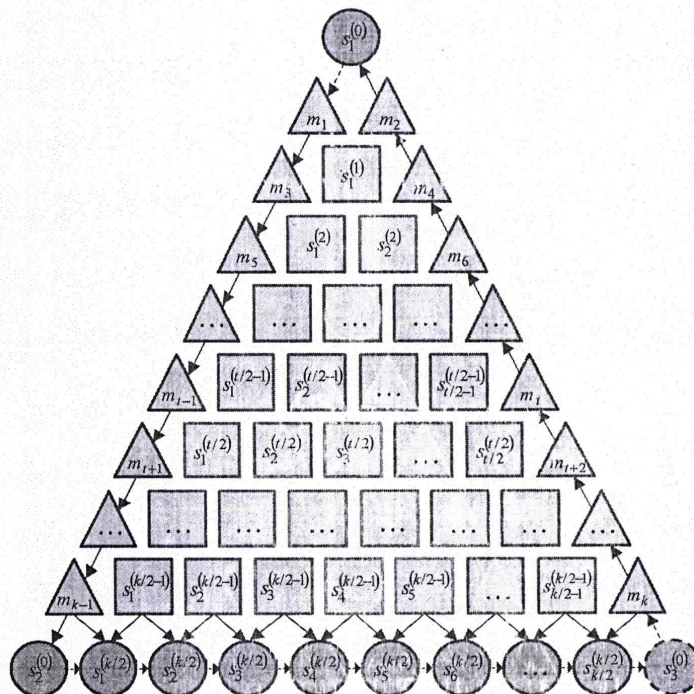
40

45

1

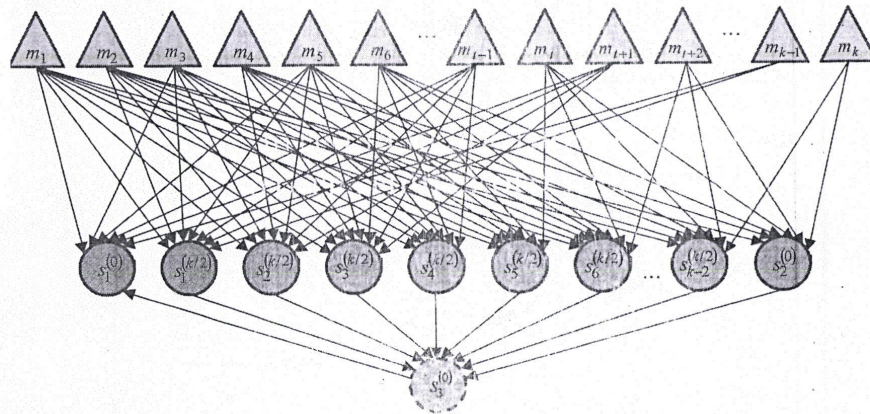


2



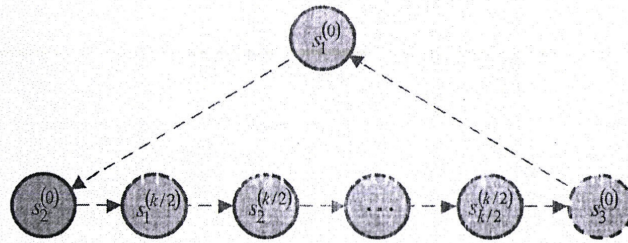
Общая схема применения хэш-функции, основанная
на правилах построения треугольника Паскаля

Фиг. 2



Общий вид сети хэширования для схемы применения хэш-функции

Фиг. 3



Фиг. 4

Схема контроля целостности эталонных хэш-кодов



