УДК 004.056.55

АКТУАЛЬНЫЕ ДОСТИЖЕНИЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ В ОБЛАСТИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В.В. Сухоцкий

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь
РУП «Белэнергосетьпроект», г. Минск, Республика Беларусь

Аннотация. В данной статье рассматриваются основные достижения в области криптографической защиты информации. Приводятся новые математические способы решения некоторых проблем контроля целостности.
Ключевые слова: достижения, контроль целостности, криптографическая защита информации.

CURRENT ADVANCES IN INTEGRITY CONTROL IN CRYPTOGRAPHIC INFORMATION PROTECTION

V.V. Sukhotski

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus
RUE "Belenergosetproekt", Minsk, Republic of Belarus

Abstract. This article examines key advances in cryptographic information protection. New mathematical methods for solving certain integrity control problems are presented.
Keywords: advances, integrity control, cryptographic information protection.

Введение

В настоящее время криптографические алгоритмы являются одним из основных способов защиты информации. Алгоритмы применяются для защиты информации при ее использовании и хранении на компьютерах, при передаче информации по сети. Данный способ защиты может гарантировать целостность, подлинность и/или конфиденциальность. Для каждой цели предназначены определенные алгоритмы. Алгоритмы шифрования используются для защиты конфиденциальности, алгоритмы формирования электронной цифровой подписи – для защиты целостности информации, алгоритмы идентификации – для проверки подлинности

источника данных. Из-за того, что методы нарушения конфиденциальности, целостности и подлинности информации часто меняются и число их растет, меняются требования к криптографическим алгоритмам и подходы к их использованию.

Основная часть

Использование таких разделов математики, как высшая алгебра и функциональный анализ, являются приоритетными в разработке криптографических алгоритмов для проверки целостности передаваемого сообщения. К одним из последних разработок относятся следующие:

1) код Рида-Соломона (недвоичный циклический код, позволяющий исправлять ошибки в блоках данных; изобретен в 1960 году сотрудниками лаборатории Линкольна Массачусетского технологического института Ирвингом Ридом и Густавом Соломоном);

2) правила построения геометрических кодов;

3) правила построения фрактала.

Первый алгоритм, используя средства высшей алгебры и функционального анализа, позволяет произвести проверку целостности информации и выявить ее нарушение, если таковое произошло. Алгоритм позволяет обрабатывать многомерные массивы.

При использовании второго алгоритма обнаружение и локализация ошибки в подблоках m_1, m_2, …, m_k блока данных M обеспечиваются посредством вычисления системы значений хэш-функции (функция, отображающая блоки произвольного размера бит исходных данных в строки бит фиксированной длины) от совокупности подблоков данных, и ее сравнения с эталонной системой, при этом блок данных M для осуществления контроля целостности представляется в виде трехмерной матрицы. К данному блоку применяется хэш-функция по правилам построения геометрических кодов, при которых блоки данных, подлежащие защите, размещены в трехмерном кубе. Контроль целостности блока данных осуществляется путем сравнения значений хэш-функции, вычисленных при запросе на использование данных, подлежащих защите, и эталонных значений хэш-функции, вычисленных ранее.

В третьем алгоритме обнаружение и локализация данных с признаками нарушения целостности блока данных M, фрагментируемого на целевые блоки, расположенные на боковых ребрах треугольника, обеспечиваются посредством вычисления группы значений хэш-функции по правилам построения треугольника Паскаля и их сравнения с эталонными. Порядок вычисления значений хэш-функции и промежуточных результатов преобразований основан на правилах построения треугольника Паскаля, полученные значения размещают

в таблице, имеющей треугольную форму. По боковым сторонам полученного треугольника последовательно размещены промежуточные результаты преобразований, вычисляемые от блоков данных, подлежащих защите. На нижней стороне треугольника размещены блоки, предназначенные для обнаружения и локализации данных с признаками нарушения целостности. Блоки содержат значения хэш-функции h, для вычисления которых используются блоки данных, подлежащих защите, и результаты промежуточных преобразований нижнего уровня.

Заключение

Были изучены методы контроля целостности информации с применением разделов прикладной математики и линейной алгебры, которые позволяют более гибко настраивать криптографические алгоритмы для решения определенных проблем передачи информации. Данные методы характеризуются способностью локализовать подблоки данных с признаками нарушения целостности и сокращением избыточности вводимых контрольных данных.

Список использованных источников

1. Стариков Т.В., Сопин К.Ю., Диченко С.А., Самойленко Д.В., Сухов А.М., Брянцев А.В. и др. Способ контроля целостности многомерных массивов данных на основе правил построения кода Рида-Соломона // Google Patents. [Электронный ресурс]. – Режим доступа: https://patentimages.storage.googleapis.com/75/87/45/f366e3b74d0b9d/RU2785862C1.pdf

2. Диченко С.А., Самойленко Д.В., Финько О.А., Фадеев Р.В., Кись С.А., Брянцев А.В. и др. Способ контроля целостности данных на основе правил построения геометрических кодов // Google Patents. [Электронный ресурс]. – Режим доступа: https://patentimages.storage.googleapis.com/a5/4f/25/f54e4dd4323c46/RU2758194C1.pdf

3. Сопин К.Ю., Новиков П.А., Диченко С.А., Самойленко Д.В., Финько О.А. Способ криптографического контроля целостности данных на основе правил построения фракталов // Google Patents. [Электронный ресурс]. – Режим доступа: https://patentimages.storage.googleapis.com/cf/5f/ac/06f89ada74cff0/RU2826863C1.pdf

References

1. Starikov T.V., Sopin K.Y., Dichenko S.A., Samoylenko D.V., Sukhov A.M., Bryancev A.V., et al. Method for control of integrity of multimeric data arrays based on reed-solomon code building rules // Google Patents. [Electronic resourse]. – Mode of access: https://patentimages.storage.googleapis.com/75/87/45/f366e3b74d0b9d/RU2785862C1.pdf

2. Dichenko S.A., Samoylenko D.V., Finko O.A., Fadeev R.V., Kis S.A., Bryancev A.V., et al. Method for monitoring data integrity based on the rules for constructing geometric codes // Google Patents. [Electronic resourse]. – Mode of access: https://patentimages.storage.googleapis.com/a5/4f/25/f54e4dd4323c46/RU2758194C1.pdf

3. Sopin K.Y., Novikov P.A., Dichenko S.A., Samoylenko D.V., Finko O.A. Method for cryptographic data integrity control based on fractal construction rules // Google Patents.

[Electronic resourse]. – Mode of access: https://patentimages.storage.googleapis.com/cf/5f/ac/06f89ada74cff0/RU2826863C1.pdf.

Сведения об авторе

Сухоцкий В.В., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»; специалист, РУП «Белэнергосетьпроект», such998slava@outlook.com.

Information about the author

Sukhotski V.V., student of the Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics"; specialist, RUE "Belenergosetproekt", such998slava@outlook.com.