

А. Д. Анкуда
(БГТУ, Минск)

РЕАЛИЗАЦИЯ И АНАЛИЗ ХЭШ-ФУНКЦИИ НА ОСНОВЕ ТРЕХСЛОЙНОЙ ХАОТИЧЕСКОЙ НЕЙРОСЕТИ

Предоставленная в работе хэш-функция на базе трехслойной хаотической нейросети в качестве сжимающего блока используется сама сеть. В качестве передаточной функции используется кусочно-линейное хаотическое отображение, обладающее всеми свойствами динамических систем детерминированного хаоса. Три составляющих её слоя реализуют перемежение, диффузию и пространственное сжатие данных.

Перед началом хэширования производится дополнение сообщения до необходимой длины по алгоритму Меркле-Дамгаарда. Реконфигурация весовых коэффициентов производится посредством псевдослучайного «генератора ключей». На первом шаге он инициализируется ключом пользователя (или предопределенными значениями в версии без ключа пользователя), на последующих шагах – выходным значением нейросети, для каждого блока сообщения. Выходное значение нейронной сети для последнего блока представляет собой дайджест всего сообщения [1]. Описанная схема хэширования представлена на рис. 1.

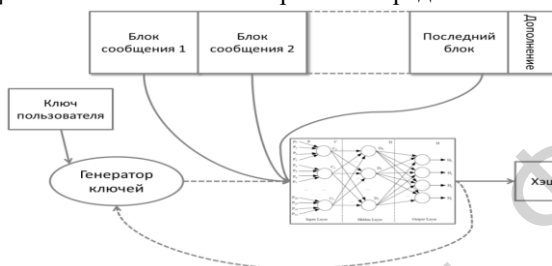


Рисунок 1 – Блочная схема хэширования

Реализованный алгоритм удовлетворяет основным требованиям криптографической стойкости для хэш-функций: стойкость к восстановлению прообраза, стойкость к коллизиям первого рода, стойкость к коллизиям второго рода.

Литература

1. Yantao, Li. A novel Hash algorithm construction based on chaotic neural network / Yantao Li, Di Xiao, Shaojiang Deng // Neural Comput&Applic, Springer-Verlag London Limited. – 2010. – P. 133–141