УДК 004.021

В. П. Семеренко, П.В.Ширшова

РАЗРАБОТКА ХЭШ-ФУНКЦИИ НА ОСНОВЕ ТЕОРИИ ЛИНЕЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТНОЙ МАШИНЫ

В связи с проведением в 2007-2011 годах открытого мирового конкурса на новый стандарт хеш-функции, актуальным является исследование новых принципов их построения, в частности, в рамках поточного шифрования.

Предлагается новый метод построения быстродействующей и надежной хэш-функции на основе теории линейной последовательностной машины (ЛПМ). В этом случае под воздействием последовательности X символов входного сообщения длины m ЛПМ из некоторого начального состояния $S(0)$ перейдет в состояние $S(m)$. Значение функции хэширования – n-разрядный код состояния $S(m)$ – является результатом сжатия последовательности X в последовательность символов длины $n\,(n<m)$.

Проведено исследование соответствия предлагаемой хэш-функции всем необходимым критериям. Такая функция будет являться однонаправленной и стойкой к коллизиям, если для ее получения используется ЛПМ с примитивным порождающим полиномом. Для повышения стойкости хэш-функции к потенциально возможным криптоатакам предложены способы, использующие свойство управляемости ЛПМ. Хэш-функция будет стойкой в смысле обращения только при использовании секретного ключа, добавляемого к передаваемому сообщению в заданных местах. Наличие секретного ключа позволяет также выполнять задачу аутентификации передаваемых сообщений. Для дальнейшего повышения криптостойкости хэш-функции предлагается использование многоканальной ЛПМ и нелинейных булевых функций [1].

Рассматривается также взаимосвязь между задачами технической диагностики и криптографии. В обоих случаях стоит задача проверки достоверности некоторых информационных данных большого объема с помощью контрольных данных значительно меньшего объема: в технической диагностике – с помощью сигнатур, а в криптографии – с помощью хэш-функций. Для решения похожих задач применяется один и тот же математический аппарат – теория ЛПМ, что позволяет использовать ранее полученные теоретические результаты сигнатурного анализа к разработке хэш-функций.

Литература

1. Семеренко В.П., Степанишин Ю.В., Гаєвський М.Л. Потокове шифрування на основі теорії лінійної послідовнісної машини. // Інформаційні технології та комп'ютерна інженерія. – 2007. №3. – С.86-93.