О.Г. Король, С.П. Евсеев

Харьковский национальный экономический университет, Харьков

МЕТОД УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ НА ОСНОВЕ МОДУЛЯРНЫХ ПРЕОБРАЗОВАНИЙ

Методы и алгоритмы ключевого хеширования информации являются областью интенсивных исследований во всем мире [1, 2], на их основе формируются наиболее перспективные механизмы обеспечения целостности и аутентичности данных в компьютерных системах и сетях. В тоже время на сегодняшний день не разработаны математические модели и методы универсального хеширования информации с высокими показателями криптографической стойкости, в том числе, обладающими свойствами доказуемо стойких криптографических систем, не разработаны вычислительные алгоритмы ключевого хеширования, задача бесключевого чтения которых сводится к решению одной из извест-

ных теоретико-сложностных задач в криптографии. Следовательно, разработка математических моделей, методов и алгоритмов ключевого хеширования для обеспечения целостности информации в компьютерных системах и сетях является перспективным направлением исследований.

Проведенные исследования показали, что применение модулярных преобразований позволяет строить схемы безопасного универсального хеширования. Использование хорошо апробированного математического аппарата модулярных преобразований позволяет обеспечить доказуемый уровень безопасности, который основан на сведении задачи нахождения прообраза и/или секретного ключа хеширования к решению одной из известных теоретико-сложностных задач, например, к задаче факторизации, дискретного логарифмирования или задаче RSA.

На основе полученных результатов проведенных исследований разработан метод доказуемо стойкого ключевого универсального хеширования с использованием модулярных преобразований. В ходе работы были проведены исследования различных вариантов построения цикловых функций, использующих модулярные преобразования. Проведенные исследования показали, что для построения универсального хеширования информации с доказуемым уровнем безопасности следует использовать цикловую функцию модульного возведения в степень. При выполнении соответствующих ограничений на параметры такого преобразования итеративное формирование хеш-кодов позволяет с одной стороны обеспечить выполнение условий модели доказуемой безопасности, т.е. высокую криптографическую стойкость, с другой стороны – обеспечить выполнение условий универсального хеширования, т.е. высокие коллизионные свойства схемы хеширования. Платой за достижение таких свойств хеширования является сравнительно высокая вычислительная сложность формирования хеш-кодов.

В работе выработаны практические рекомендации по аппаратной и программной реализации предлагаемой схемы хеширования. Разработана программная модель схемы универсального хеширования, которая практически реализует предложенные алгоритмы и позволяет проводить статистические исследования коллизионных свойств, получать численные оценки по соответствующим критериям и показателям эффективности. Для снижения вычислительной сложности реализации схем хеширования предлагается использовать алгоритм быстрого возведения в степень, позволяющий эффективно вычислять значения цикловых функций.

Список литературы

1. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag.

2. Handbook of Applied Cryptography [Электронный ресурс] / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – Режим доступа к ресурсу: http://www.cacr.math.uwaterloo.ca/hac.