ПРОГРАММНЫЕ СРЕДСТВА ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ

Отрыванкина Т.М., Благовисная А.Н.
Оренбургский государственный университет, г. Оренбург

Аппарат теории булевых функций является одним из важнейших математических инструментов, применяемых в современных криптосистемах. Булевы функции служат структурными элементами блочных, поточных шифров, а также широко известных криптографических хэш-функций. Исследования в области современной прикладной математики, имеющие целью совершенствование криптографических средств, являются актуальными и востребованными, поэтому необходимо отражать это научное направление в учебных курсах, посвященных криптографическим средствам защиты информации.

Булевы функции представляют собой сложный и многогранный объект исследований в современной математике. Одной из важных задач преподавания криптографии является выбор тех математических средств и методов теории булевых функций, которые необходимы для понимания математических основ этой дисциплины. Кроме математических аспектов содержания разделов учебных дисциплин, посвященных математическим методам защиты информации, не менее актуальной является проблема выбора программных средств, позволяющих исследовать криптографические свойства булевых функций.

Одним из вариантов решения проблемы выбора программного средства может быть создание студентами собственных инструментов для исследования свойств булевых функций. Этот подход возможен при достаточном учебном времени, отводимом студентам на выполнение лабораторных работ по криптографическим булевым функциям. Другой вариант – применение готовых программных продуктов для изучения криптографических характеристик булевых функций. Оба подхода скорее не исключают, а даже дополняют друг друга. Существующие программные модули написаны программистами-практиками на различных языках программирования и в различных средах, имеют собственный интерфейс и отражают авторский подход к решению проблем программирования задач теории криптографических булевых функций. Использование таких программных модулей, их изучение позволяют студентам совершенствовать навыки создания собственных программ.

Рассмотрим некоторые программные средства работы с криптографическими булевыми функциями. В силу актуальности исследований в области криптографии в целом и в теории криптографических булевых функций, в частности, такие программы появляются и совершенствуются в зависимости от потребностей теории и практики применения криптографических методов защиты информации.

В работе [1] описывается система для работы с булевыми функциями Boolean Functions. Она представляет собой библиотеку классов и функций на

языке C++. Согласно описанию данной системы пользователь может работать с двоичными векторами и совершать стандартные операции над ними: определение веса Хэмминга, сложение двух векторов, вычисление их скалярного произведения, сравнение двух векторов и др. По словам создателей системы Boolean Functions, библиотека работает с представлениями булевой функции в виде АНФ, таблицы истинности и представлением с помощью следа, умеет переводить одно представление в другое. Boolean Functions позволяет проверять, являются ли две булевы функции аффинно эквивалентными, и генерировать функции, аффинно эквивалентные заданной. Данная система позволяет работать с функциями специального вида, например, с бент-функциями: выполнять проверку, является ли заданная функция бент-функцией, генерировать бент-функции, строить коды, основанные на аппарате бент-функций.

В статье [2] представлен класс VBF, также написанный на языке программирования C++ и предназначенный для анализа векторных булевых функций с криптографической точки зрения. Данный класс создан на основе библиотеки теории чисел NTL, реализованной Виктором Шоупом. В нем заменены некоторые модули общего назначения более подходящими для криптографии, а также добавлены новые модули. Этот класс позволяет получать как классические представления векторной булевой функции в виде таблиц истинности и алгебраических нормальных форм, так и полиномиальное представление векторной булевой функции над $GF(2^n)$. С помощью рассматриваемого класса возможно вычисление таких математических характеристик, как спектр Уолша, линейный профиль, дифференциальный профиль и спектр автокорреляции. С помощью класса VNB можно находить такие криптографические критерии, как нелинейность, линейное расстояние, порядок корреляционного иммунитета, сбалансированность, алгебраическую степень, критерии распространения, а также ряд других криптографических характеристик.

Анализ возможностей системы Boolean Functions и класса VBF позволяет сделать вывод, что они удобны для пользователей-программистов, однако не ориентированы на человека, впервые изучающего аппарат теории криптографических булевых функций. Тем не менее, рассмотренные программные средства могут быть рекомендованы к изучению и использованию студентам, хорошо владеющим навыками программирования на языке C++.

Кроме классов и систем работы с булевыми функциями, реализованными на языке C++, встречаются описания программных модулей, созданных и на других языках программирования. Например, в работе [3] рассмотрен пакет boolfun, написанный на языке R. Пакет boolfun реализует методы, позволяющие находить ряд криптографических характеристик булевых функций. Применение данного пакета полезно при исследовании криптографических характеристик булевых функций, однако его инструменты не предусматривают вывода промежуточных результатов вычислений,

характеризующих свойства функций. Важным достоинством как пакета boolfun, так и среды, в которой пакет разработан, является его доступность, так как рассматриваемые программные продукты относятся к свободному программному обеспечению. Однако использование пакета boolfun на учебных занятиях затруднительно в силу того, что студенты, как правило, не знакомы ни со средой, ни с языком программирования R. Вариантом применения пакета boolfun в учебном процессе может быть его самостоятельное освоение и использование студентами в курсовых, выпускных квалификационных работах, а также в студенческих научных исследованиях.

Следует отметить, что помимо программных средств, узко ориентированных на работу с криптографическими характеристиками булевых функций, существуют различные программные средства общего назначения, позволяющие на том или ином уровне сложности реализовать работу с булевыми функциями. К наиболее универсальным и интуитивно понятным в использовании можно отнести математические пакеты, такие, как Mathematica, Maple, Matlab. Имея широкий спектр возможностей, они позволяют организовать работу и с булевыми функциями, но для решения учебных задач криптографии необходимо иметь хорошие навыки работы с системами компьютерной математики, а также уметь создавать вспомогательные функции или писать специальные программы, используя средства среды математических пакетов.

В заключение отметим, что разработка и создание программных продуктов, позволяющих исследовать криптографические булевы функции, как правило, не ориентировано на их применение в учебном процессе. Тем не менее, они обладают образовательным потенциалом, что позволяет при определенных условиях применять их в учебной деятельности.

Список литературы

1. Коломеец, Н.А. Boolean Functions – система для работы с булевыми функциями / Н.А. Коломеец, А.В. Павлов // Вычислительные методы в дискретной математике. Приложение. – 2011. – №4. – С. 67-68.

2. Álvarez-Cubero, J.A. A C++ Class for analyzing Vector Boolean functions from a cryptographic perspective [Электронный ресурс] / J.A. Álvarez-Cubero, P.J. Zufiria // International Conference on Security and Cryptography (SECRYPT). – 2010. – Режим доступа: http://oa.upm.es/8149/1/INVE_MEM_ 2010_1430.pdf. – 10.12.2014.

3. Lafitte, F. Cryptographic Boolean Function with R / F. Lafitte, D.Van Heule, J. Van Hamme // The R Journal. – 2011. – V. 3/1. – P. 44-47.