Разработка и исследование методов обфускации для информационной защиты программ и схем

Руководитель проекта
профессор, д.ф.-м.н. Н.Н. Кузюрин,

Ответственный исполнитель
Зав. лаб. ОВТ КИН, к.ф.-м.н. А. В. Николаев

Московский физико-технический институт
(государственный университет)

Обфускация – это преобразование программы к такому виду, при котором

1. Функциональные возможности исходной программы сохраняются;
2. Сложность и эффективность полученной программы ухудшаются незначительно;
3. Извлечение полезной информации об устройстве алгоритмов и структур данных становится вычислительно трудной задачей.

2-ое полугодие 2007

Техническое задание

1. Исследовать задачу обфускации микросхем;
2. Предложить критерии стойкости обфускации схем относительно угроз и атак различного вида;
3. Выделить классы программ и схем, допускающих стойкую обфускацию;
4. Выделить криптографические задачи, к которым сводится проблема обфускации программ;
5. Разработать новые методы обфускации программ на основе установленной сводимости;
6. Разработать методы кодирования данных для проведения защищенных вычислений алгебраических и логических функций схемами.

2-ое полугодие 2007

Полученные результаты

1. Проведен анализ типичного маршрута проектирования микроэлектронных схем.

   Предложена формальная постановка задачи обфускации микроэлектронных схем;

   Для каждого этапа проектирования исследована безопасность и стойкость применения ранее предложенных обфускирующих преобразований программ для информационной защиты микроэлектронных схем.

Отчет, раздел 2

2-ое полугодие 2007

Полученные результаты

2. Предложены 3 новых критерия стойкости обфускирующих преобразований (модель «виртуального серого ящика», сокрытие алгоритма, сокрытие константы).

   Доказана невозможность построения стойкого обфускатора в модели «виртуального серого ящика».

   Доказана возможность стойкой обфускации конечных автоматов, скрывающей алгоритм вычисления.

Отчет, раздел 3

2-ое полугодие 2007

Полученные результаты

3. Разработаны 2 новых метода обфускации микроэлектронных схем:
   — обфускация с разделением схем,
   — обфускация с использованием пароля;

   Проведена оценка стойкости предложенных обфускирующих преобразований и издержек, связанных с их применением.

   Описаны классы комбинационных логических схем, к которым применимы предложенные методы обфускации.

Отчет, раздел 4

2-ое полугодие 2007

Полученные результаты

4. Исследованы криптографические задачи и методы, к которым может быть сведена проблема обфускации микроэлектронных схем:

   — генерация псевдослучайных последовательностей,

   — шифрование с секретным ключом,

   — алгоритм Мак-Эллиса шифрования с открытым ключом;

   — алгоритм шифрования с открытым ключом на основе задачи об укладке ранца.

Отчет, разделы 4, 5

2-ое полугодие 2007

Полученные результаты

5. Предложен новый метод информационной защиты постоянных запоминающих устройств (ПЗУ), использующий генераторы псевдослучайных последовательностей и шифр Вернама;

   Установлено, что применение алгоритма шифрования Мак-Эллиса повышает стойкость метода обфускации с разделением схемы;

   Предложен новый метод обфускации программ, использующий хэш-функции и алгоритмы шифрования на основе задачи об укладке ранца.

Отчет, разделы 4, 5

2-ое полугодие 2007

Полученные результаты

6. Разработан новый метод эквивалентных преобразований алгебраических схем, позволяющий конструировать стойкие схемы гомоморфных вычислений над зашифрованными данными;

   Проведен анализ применимости известных криптосистем (RSA, Эль-Гамаля, Пэйе и др.) для построения схем гомоморфных вычислений.

Отчет, разделы 6

Виды реализации научно-технических результатов работ в 2007 г.	
1. Кандидатские диссертации	1
2. Публикации в ведущих научных журналах	4
3. Учебные пособия	1
4. Курсы лекций	1
5. Дипломные работы	2

Список исполнителей по проекту

Руководитель проекта

- Кузюрин Николай Николаевич, д.ф.-м.н., профессор ФУПМ МФТИ

Ответственный исполнитель

- Николаев Андрей Валентинович, к.ф.-м.н., зав. лаб. ОВТ КИН МФТИ

Исполнители (совместители):

- Захаров Владимир Анатольевич, к.ф.-м.н., доцент ФУПМ МФТИ
- Шокуров Александр Владимирович, к.ф.-м.н., доцент ФУПМ МФТИ
- Фомин Станислав Александрович, м.н.с. ФУПМ МФТИ
- Несов Владимир Сергеевич, аспирант ФУПМ МФТИ
- Гетьман Александр Игоревич, аспирант ФУПМ МФТИ
- Жук Сергей Николаевич, аспирант ФУПМ МФТИ

Публикации по проекту

Статьи:

1. Н.П. Варновский, В.А. Захаров, Н.Н. Кузюрин, А.В. Шокуров. Современные методы обфускации программ: классификация и сравнительный анализ. Известия ЮФУ, 2007, N 1, с. 93-98.
2. В.С. Несов, Использование побочных эффектов функций для ускорения автоматического поиска уязвимостей в программах, Известия ЮФУ, 2007, N 1, с. 134-138.
3. В.А. Захаров, Е.В. Костылев. О сложности задачи антиунификации. Дискретная математика, 2008, т. 20, N 1.
4. N.N. Kuzurin, A.V. Shokurov, N.P. Varnovsky, V.A. Zakharov. On the concept of software obfuscation in computer security. Lecture Notes in Computer Science, v. 4779, 2007, p. 281-298.

Монография

Н.Н. Кузюрин, С.А. Фомин, «Эффективные алгоритмы и сложность вычислений», 313 с., М., МФТИ, 2007 г.

Кандидатская диссертация:

Маликов О. Р. «Исследование и разработка методики автоматического обнаружения уязвимостей в исходном коде программ на языке Си»