Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК _____

Захарченко
Константин Владимирович

Шифрование сообщений в протоколах интерактивных доказательств

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-40 80 02 Системный анализ, управление и обработка информации

_____

Научный руководитель
Кукин Дмитрий Петрович
Кандидат технических наук, доцент

_____

Минск 2017

Библиотека БГУИР

КРАТКОЕ ВВЕДЕНИЕ

Исследование классических криптографических конструкций, таких как протокол интерактивного Доказательства с Нулевым Разглашением в нестандартных моделях среды, как, например, в модели со сбросом, является важной задачей, необходимой для развития научной области криптографии. Другой важной задачей исследователя является анализ и применение новых криптографических конструкций с целью определения границ возможностей этих конструкций и их потенциала при решении задач построения стандартных криптографических схем. Так каждый год появляются новые примитивы, использующие последние разработки и доказательства в области криптографии. Один из таких примитивов – Шифрование со Свидетельством, представляет большой пласт криптографических конструкций, называющихся Функциональное Шифрование. В диссертационной работе рассматривается применение такого варианта Шифрования со Свидетельством, как Псевдослучайные Функции со Свидетельством. Актуальным является вопрос применимости этого примитива для построения стандартных криптографических конструкций.

Что касается протокола интерактивного Доказательства с Нулевым Разглашением, важно проанализировать пути к наиболее оптимальной реализации этого примитива. Со времени появления в литературе модели со сбросом для интерактивных протоколов было продемонстрировано немало различных конструкций, реализующих протокол Доказательства с Нулевым Разглашением с сохранением свойств безопасности и полноты в этой модели. Однако работа по нахождению минимального количества раундов этого интерактивного протокола, которых было бы достаточно, чтобы произвести доказательство, до сих пор актуальна. Так в данной работе продолжается исследование на тему построения целевого протокола в минимальное количество раундов. Актуальность модели со сбросом заключается в том, что последнее время всё чаще при практической реализации криптографических устройств возникает ситуация, когда одна или несколько взаимодействующих сторон представлены достаточно простыми в техническом плане модулями, в которых некоторые необходимые для безопасности конструкции требования могут быть неудовлетворительны. Так как некоторые криптографические схемы реализуются на смарт-картах, микросхемах и других устройствах, имеющих ограниченную или порой отсутствующую постоянную память, а также трудности с организацией надёжного источника случайных данных, модель со сбросом имеет далеко не теоретический интерес.

Подводя итог, можно сказать, что данная работа занимается исследованием, актуальным по трём различным причинам. Первая – это анализ новой

Библиотека БГУИР

криптографической конструкции, Шифрования со Свидетельством. Вторая – это построение протокола Доказательства с Нулевым Разглашением в количество раундов, меньшее, чем в предыдущих литературных источниках. Третья – это применение к конструирующимся примитивам модели со сбросом, актуальной в последнее время.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью исследования является построение двухраундового протокола Доказательства с Нулевым Разглашением в модели со сбросом. При этом важно сохранить свойство полноты, гарантирующее возможность выполнения доказательства верного утверждения, свойство безопасности, гарантирующее невозможность доказательства ложного утверждения и свойство нулевого разглашения, гарантирующее отсутствие утечки информации о доказывающем утверждении.

Задачи, поставленные для достижения заданной цели, включают в себя:

1. Анализ возможностей реализации целевой конструкции в заданных условиях.
2. Построение извлекаемого Обязательства с функцией трудного бита.
3. Построение схемы Шифрования со Свидетельством и Псевдослучайных Функций со Свидетельством.
4. Применение схемы Псевдослучайных Функций со Свидетельством и схемы симметричного шифрования для построения конструкции Шифрования с Обязательством, представляющей из себя забывчивую передачу со свойством идеального скрытия данных принимающей стороны.
5. Анализ возможностей злонамеренного участника протокола интерактивного доказательства с нулевым разглашением, использующего атаку со сбросом.
6. Анализ уязвимости протокола Блюма при осуществлении атаки со сбросом с целью построения безопасного варианта протокола.
7. Применение схемы Шифрования с Обязательством с целью построения двухраундового варианта классического протокола Блюма безопасного в модели со сбросом.
8. Применение модели белого ящика для построения симулятора с целью демонстрации наличия свойства нулевого разглашения у сконструированного протокола доказательства с нулевым разглашением.
9. Анализ сконструированного протокола в условиях атаки со сбросом.

Объектом исследования является протокол Доказательства с Нулевым Разглашением в модели со сбросом.

Библиотека БГУИР

Предметом исследования является задача построения двухраундового протокола Доказательства с Нулевым Разглашением в модели со сбросом с использованием Шифрования со Свидетельством.

Теоретическая значимость работы заключается в определении понятия трудного бита для схемы Обязательства и демонстрации возможности использования схемы Обязательства с трудным битом совместно со схемой Псевдослучайных Функций со Свидетельством для построения схемы забывчивой передачи. Это построение позволяет исследовать функциональные возможности новой криптографической конструкции – Псевдослучайных Функций со Свидетельством. Так же теоретическая значимость работы состоит в демонстрации первого *двухраундового* протокола Доказательства с Нулевым Разглашением, сохраняющего свойства безопасности в модели со сбросом.

Практическая значимость работы состоит в том, что рассматриваемая модель со сбросом последнее время достаточно актуальна при реализации криптографических схем на практике. И так как, протоколы Доказательства с Нулевым Разглашением применяются во множестве практических криптографических конструкций, таких как, схема аутентификации, электронное голосование, электронная коммерция и прочие, представленная конструкция, предлагающая меньшее количество раундов, позволяет уменьшить верхнюю границу на количество раундов во многих практических конструкциях.

Результаты, приведённые в диссертации, получены соискателем лично. Вклад научного руководителя Д. П. Кукина, заключается в формулировке целей и задач исследования.

Основные положения диссертационной работы докладывались и обсуждались на 52-й научной конференции аспирантов, магистрантов и студентов, “Информационные технологии и управление” (Минск, 23-25 апреля 2016 г.).

По теме диссертации опубликована 1 печатная работа, в том числе 1 работа в сборнике трудов и материалов конференции БГУИР.

Диссертация состоит из введения, трёх глав, заключения, списка использованных источников и списка публикаций автора. В первой главе представлен анализ предметной области, приведены основные результаты по теме, опубликованные в литературе. Вторая глава содержит необходимые теоретические выкладки, описания требований к конструируемым схемам. Третья глава содержит описание построений целевых схем и протоколов. Производится анализ полученных конструкций, демонстрируются необходимые свойства.

Общий объём работы составляет 65 страниц, из которых основного текста 57 страниц, 2 рисунка, список использованных источников из 56 наименований на 5 страницах.

Библиотека БГУИР

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность диссертационной работы, приведена цель и основные задачи работы, кратко дана информация об истории и текущем состоянии проблемы.

В первой главе "Обзор теоретических моделей и ограничений" приведено описание основных литературных источников, задающих область знаний, рассматриваемую в диссертационной работе. Так в начале главы рассматриваются истоки появления модели белого ящика. Для этого описывается понятие симулятора для интерактивных протоколов. Даны ссылки на основные работы, показывающие ограничения симулятора в модели чёрного ящика. Рассмотрены наиболее важные статьи, демонстрирующие различные варианты реализации модели белого ящика. Для всех освещаемых понятий приводится связь с проблемами, рассматриваемыми в текущей работе. Так в диссертации за основу модели симулятора берётся вариант белого ящика.

Далее приводится история развития проблемы атаки со сбросом в протоколах доказательств. Приводятся ссылки на литературные источники, освещающие проблему параллельного доказательства и последующие за ними источники, занимающиеся вопросом сбрасываемого доказательства. Рассматривается дальнейший путь развития этих понятий, выразившийся в появлении модели со взаимным сбросом. Именно модель со взаимным сбросом принимается в данном диссертационном исследовании, как модель среды для проектируемого протокола.

Чтобы продемонстрировать актуальность текущей работы, приводится анализ литературы на имеющиеся оценки нижних границ количества раундов проектируемого протокола. Так показывается, что разработанный протокол имеет меньшее количество раундов, чем предыдущие аналоги. Демонстрируется связь между проблемой невозможности идеальной обфускации и построением симулятора для протокола интерактивного доказательства в модели белого ящика.

Отдельная часть первой главы посвящена обзору литературы, в которой внимание уделено схеме Шифрования со Свидетельством. Освещена статья, которая впервые продемонстрировала этот примитив. Указаны литературные источники, занимающиеся проблемой практической реализации и оптимизации в вычислительном плане Шифрования со Свидетельством. Рассмотрено более строгое определение этого примитива – Извлекаемое Шифрование со Свидетельством. Именно такое определение необходимо для нужд данной диссертационной работы. Как завершение рассмотрения пути возникновения примитива Шифрования со Свидетельством, приведён обзор Псевдослучайных Функций со Свидетельством – более удобной на практике схеме.

Библиотека БГУИР

Заканчивается первая глава работы приведением ссылок на работы, сравнивающие Извлекаемые Функции и Неразличимую Обфускацию. Для данной диссертации проблема состоит в том, что нет однозначных доказательств корректности и безопасности и используемых конструкций. К тому же именно Неразличимая Обфускация – это криптографическая схема, возможность существования которой противоречит надёжности используемых в работе конструкций. Это противоречие рассматривается в заключительной части первой главы работы.

Во второй главе "Определения и требования безопасности. Шифрование с Обязательством" даны все необходимые определения, приведены требования к проектируемым конструкциям, дано определение схемы Шифрования с Обязательством, вводимой в данной работе.

Начинается глава с описания определений простых криптографических примитивов, таких как пренебрежимо малая функция, симметричное шифрование, схема Обязательства, освещены некоторые базовые понятия из теории формальных языков, что будет необходимо для описания схемы Псевдослучайных Функций со Свидетельством. Для схемы Обязательства в данной работе введено понятие трудного бита. Ранее это понятие определялось только для односторонних функций.

С целью использования формальных определений, приводятся необходимые теоретические выкладки на тему интерактивных протоколов. Вводится определение свойств нулевого разглашения, полноты и безопасности для интерактивных протоколов. Описывается модель со сбросом. Глава заканчивается формальным описанием схемы Шифрования со Свидетельством и введением определения схемы Шифрования с Обязательством.

В третьей главе "Построение и анализ целевых схем" приводится описание практической реализации целевого протокола и необходимых для этого криптографических конструкций. Так в начале описывается построение Шифрования со Свидетельством, обосновывается выбор схемы симметричного шифрования. Однако таким конструкциям не уделяется много внимания по причине исключительно малого количества вклада автора диссертации в построение этих примитивов.

В продолжении главы большее внимание получает конструирование схемы Обязательства. Производится построение схемы Обязательства на основе уже существующей схемы, но с использованием односторонней функции, основывающейся на умножении в поле точек эллиптической кривой. Демонстрируются необходимые свойства полученной схемы Обязательства, а именно извлекаемость и наличие функции трудного бита. В качестве завершения анализа практической реализации схемы Обязательства, производится выбор

Библиотека БГУИР

параметров эллиптической кривой.

Используя приведённые во второй главе определения из теории формальных языков, описывается язык над схемой Обязательства. Этот язык необходим для построения схемы Шифрования с Обязательством. Построение этой конструкции приводится далее с использованием разработанной схемы Обязательства, симметричного шифрования и схемы Псевдослучайных Функций со Свидетельством.

Оставшаяся часть третьей главы посвящена построению и анализу целевого протокола Доказательства с Нулевым Разглашением. Перед построением протокола приводится краткое описание протокола Блюма. Демонстрируется, как, используя приём распараллеливания протокола, можно добиться выполнения протокола Блюма в четыре раунда. Далее, основываясь на приведённом протоколе, производится построение целевого протокола, выполняемого за два раунда и обладающего всеми свойствами безопасности в модели со сбросом. С целью демонстрации наличия у спроектированного протокола свойства нулевого разглашения, производится построение алгоритма симулятора. Аргументируются свойства полноты и безопасности. Рассматривается уязвимость оригинального протокола Блюма при атаке со сбросом, аргументируется безопасность разработанного протокола при аналогичной атаке. В конце главы кратко приводятся рекомендация к реализации схемы генератора псевдослучайных чисел.

ЗАКЛЮЧЕНИЕ

Исследуемая тема проработана в полной мере, были исследованы литературные источники начиная с истоков зарождения области Доказательств с Нулевым Разглашением и заканчивая анализом докладов, представленных на ведущих криптографических конференциях последних лет. Была проанализирована возможность реализации целевой конструкции. Для того, чтобы поддержать возможность использования симулятора в модели белого ящика, была разработана схема Обязательства со свойством извлекаемости и функцией трудного бита. Была продемонстрирована конструкция такой схемы Обязательства, основывающаяся на односторонней функции в поле точек эллиптической кривой.

В теоретической главе была введена схема Шифрования с Обязательством. Для построения Шифрования с Обязательством, был описан вариант реализации схемы Псевдослучайных Функций со Свидетельством, основывающийся на мультилинейных отображениях и задаче суммы подмножества. Так же для конструирования Шифрования с Обязательством использовалась схема симметричного шифрования и разработанная схема Обязательства.

Библиотека БГУИР

Анализ возможностей злонамеренного участника протокола, использующего атаку со сбросом, показал, что атака со сбросом позволяет нарушить, как свойство безопасности, так и свойство нулевого разглашения протокола, спроектированного без учёта возможности атаки. Был проанализирован протокол Доказательства с Нулевым Разглашением Блюма. С целью защиты протокола Блюма от атаки злонамеренной стороны, была применена схема Шифрования с Обязательством. Полученный протокол имеет количество раундов меньшее, чем у протокола Блюма, а также меньшее, чем у других безопасных в модели со сбросом протоколов, продемонстрированных в литературе.

Используя симулятор в модели белого ящика, было показано наличие свойства нулевого разглашения у сконструированного протокола. Таким образом, в работе было продемонстрировано, как современные криптографические конструкции, такие как Шифрование со Свидетельством, мультилинейные отображения и Эллиптическая Криптография позволяют решать классические проблемы криптографии, получая более выгодный, чем было известно ранее, протокол, сохранив в то же время безопасность против достаточно мощной криптографической атаке.

Возможные сферы применения разработанной схемы Доказательства с Нулевым Разглашением включают в себя доказательство корректности вычислений в схемах, использующих гомоморфное шифрование, использование доказательства обладания каким-то секретным знанием с целью аутентификации, доказательство корректного выполнения алгоритма протокола в схемах электронного голосования. Так же Доказательство с Нулевым Разглашением используется при реализации схем разделения секрета, функционального шифрования, одноразовых программ, электронной коммерции и многих других. Предоставление конструкции, позволяющей выполнить доказательство в два раунда и при этом сохранить свойство нулевого разглашения в модели со сбросом, позволяет уменьшить верхнюю границу для количества сообщений при выполнении вышеперечисленных схем.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1 Захарченко, К. В. Шифрование с обязательством и сбрасываемое доказательство с нулевым разглашением в два раунда / К. В. Захарченко — // Информационные технологии и управление : материалы 52-й научной конференции аспирантов, магистрантов и студентов. (Минск, 23 - 25 апреля 2016 г.). — Минск : БГУИР, 2016. – С. 95 - 96.

Библиотека БГУИР