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

УДК 003.26

Еленевич
Роман Владимирович

Анализ и разработка методов и средств доверенной цифровой подписи

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Ярмолик Вячеслав Николаевич
д. т. н., профессор

Минск 2015

КРАТКОЕ ВВЕДЕНИЕ

Основными угрозами для информационной безопасности являются перехват данных с целью использования сведений закрытого характера, модификация данных с целью фальсификации передаваемой информации, уничтожение данных для нарушения нормальной работы системы. Данные виды информационных угроз представляют особую опасность для информационной среды, так как их обнаружение является сложной технической задачей. Проблемы, вызванные нарушением информационной безопасности, могут повлечь за собой финансовые потери для физических лиц и организаций в целом, а также носить стратегический характер в конкурирующей борьбе между противоборствующими сторонами. В данной ситуации необходимо использовать комплекс мер, направленных на повышение уровня защиты информационных потоков.

Одним из основных направлений защиты информации является использование криптографических средств. В криптографии существуют методы и подходы, ориентированные на обеспечение конфиденциальности, целостности и доступности информации.

Основное внимание в диссертации уделено криптографическим методам обеспечения целостности информации. Основными криптографическими методами обеспечения целостности информации являются электронные цифровые подписи, криптографические хеш-функции, коды проверки подлинности. Наиболее распространенным и мощным средством является электронная цифровая подпись.

Электронная цифровая подпись является наилучшим вариантом обеспечения целостности информации с точки зрения компромисса между простотой, защищенностью и производительностью, позволяя также решать проблемы аутентификации и неотрицания авторства.

Существует большое количество модификаций, которые помимо обеспечения целостности данных предоставляют и дополнительные свойства, имеющие большое практическое применение. Именно они и будут являться темой для исследования в данной работе. Целью данной магистерской диссертации будет являться анализ протоколов ДЦП, их программная реализация и анализ дополнительных накладных расходов на вычисления, которые необходимы для предоставления заявленных свойств. На основе полученных результатов предложить возможные пути оптимизации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является анализ и разработка методов доверенной цифровой подписи: незащищенной ДЦП с доверенностью, защищенной ДЦП с доверенностью, пороговой ДЦП.

Для решения поставленной цели необходимо решить следующие основные задачи:

1. Проанализировать свойства, которые предлагает каждая математическая модель модификации ДЦП.

2. Проанализировать математический аппарат, который позволяет получить уникальные свойства модификаций ДЦП.

3. Предложить, какие новые практические результаты модификации ДЦП позволяют получить в отличие от традиционных методов ЭЦП.

4. Показать работоспособность представленных математических моделей протоколов ДЦП, разработав программный криптографический модуль.

5. Экспериментальным путем показать накладные расходы приходятся на доверенные модификации в отличии от классической ЭЦП.

6. Экспериментальным путем показать, как влияют размеры группы и порогового значения на производительность порогового протокола ДЦП.

Областью исследования в данной работе является раздел криптосистем с открытым ключом.

Объектом исследования является электронная цифровая подпись.

Предметом исследования является изучение свойств модификаций протоколов ДЦП, таких как незащищенная ДЦП, защищенная ДЦП и пороговая ДЦП.

Практическая актуальность исследования связана с необходимостью предоставления новых свойств уже существующим реализациям ЭЦП, и необходимостью делегировать свои права на подписание документов другим лицам. Особенно актуальным является возможность делегирования прав на подписание не одной, а группе доверенных сторон.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа выполнялась в соответствии с научно-техническим заданием и планом работ кафедры «Программное обеспечение информационных технологий» по теме «Разработать модели, методы, алгоритмы для оценки параметров, повышения надежности и качества функционирования аппаратно-

программных средств систем и сетей сложной конфигурации и внедрить в современные обучающие комплексы» (ГБ № 11-2004, № ГР 20111065, научный руководитель НИР – В. В. Бахтизин).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя В. Н. Ярмолика, заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались и обсуждались на «51-ой научной конференции аспирантов, магистрантов и студентов БГУИР» (БГУИР, Минск, Беларусь, 2015) по направлению компьютерные системы и сети [1-А]; IX Международная научно-методическая конференции «Дистанционное обучение – образовательная среда XXI века» в секции 4 «Информационные компьютерные сети и системы в сфере образования» (БГУИР, Минск, Беларусь, 2015) [2-А].

Опубликованность результатов диссертации

По теме диссертации опубликовано 2 печатные работы, из них 1 работа в материалах конференции аспирантов, магистрантов и студентов БГУИР и 1 работа в сборнике трудов и материалов международной конференции.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, трех глав, заключения, списка использованных источников, списка публикаций автора и приложений.

Во введение была обоснована актуальность диссертационной работы, показана эффективность использования цифровой подписи для обеспечения целостности, аутентификации и неотрицания авторства. Показана практическая значимость доверенных протоколов.

В первом разделе проводится анализ предметной области. Были найдены источники информации, проведена оценка текущего этапа развития криптографии, в частности алгоритмов, методов и протоколов электронной цифровой подписи. Выделена и подробно рассмотрено семейство протоколов ДЦП. На основе проведенного анализа определены и сформулированы задачи к

диссертационной работе.

Во втором разделе «Математические модели» были подробно рассмотрены основные леммы и математический аппарат, на основе которого разрабатываются протоколы цифровой подписи. Основное внимание уделено математическому аппарату доверенной цифровой подписи: схема незащищенной ДЦП частичного делегирования, схема защищенной ДЦП частичного делегирования, схема пороговой ДЦП без распространения секретных частей. Проведен анализ математического аппарата, который был применен для получения заявленных свойств. Проведен анализ накладных расходов связанных с модификацией схем цифровой подписи.

Третий раздел описывает эксперименты, проведенные над различными модификациями ДЦП. Было показано, какие дополнительные затраты приходится на делегирование полномочий. Проведено сравнение производительности с существующими опубликованными тестами. Полученные результаты показывают, что доверенные модификации на основе DSA не накладывают существенных дополнительных расходов. Приведён детальный анализ производительности пороговой схемы доверенной цифровой подписи на различных этапах протокола и экспериментально показаны слабые места протокола, которые требуют доработки.

Общий объем работы составляет 89 страниц, из которых основного текста – 62 страниц, 14 рисунков на 7 страницах, 6 таблиц на 4 страницах, список использованных источников из 23 наименований на 2 страницах и 2 приложения на 26 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Пояснительная записка состоит из 4 основных разделов.

Во **введение** была обоснована актуальность диссертационной работы, показана эффективность использования цифровой подписи для обеспечения целостности, аутентификации и неотрицания авторства. Показана практическая значимость доверенных протоколов.

В **первой главе** проводится анализ предметной области. В разделе 1.1 проведено аналитическое сравнение классических криптосистем и криптосистем с открытым ключом. Были сделаны выводы о преимуществах, недостатках и областях применения.

В разделе 1.2 проведен аналитический обзор криптографических методов обеспечения целостности, аутентификации, неотрицания авторства. Проведен анализ существующих методов, их недостатики, преимущества и области применения.

В разделе 1.3 выполнен аналитический обзор стандартов и протоколов

электронной цифровой подписи.

В разделе 1.4 проведен подробный аналитический обзор протоколов доверенной цифровой подписи. Приведена классификация, принятые обозначения, требования к доверенной цифровой подписи.

В разделе 1.5 сделаны выводы на основании проведенного анализа и поставлены задачи для решения в рамках диссертационной работы.

Во **второй главе** «Математические модели» были подробно рассмотрены основные леммы и математический аппарат, на основе которого разрабатываются протоколы цифровой подписи. В разделе 2.1 приведены основополагающие знания из теории чисел, который в последующем активно используется при описании математических моделей.

В разделе 2.2 приводятся обозначения, применяемые при описании математических моделей и даётся определение некоторым обозначениям.

В разделе 2.3 приводится общая схема протокола доверенной цифровой подписи.

В разделе 2.4 приводится математическая модель предлагаемого протокола доверенной цифровой подписи частичного делегирования на основе криптосистемы ElGamal. Проанализирован математический аппарат, предоставляющий заявленные свойства, а также сделаны выводы о самых затратных по времени операциях протокола.

В разделе 2.5 приведена математическая модель рассматриваемого протокола защищённой доверенной цифровой подписи частичного делегирования с доверенностью. Проводится анализ аналогичный разделу 2.4.

В разделе 2.6 приведено краткое описание протокола пороговой доверенной цифровой подписи и предложен математический аппарат для её реализации. Проводится анализ аналогичный разделу 2.4.

В **третьей главе** описываются эксперименты, проведенные над различными модификациями ДЦП. В разделе 3.1 произведен выбор инструментов для реализации моделей в виде криптографического модуля. Проведено обоснования выбора платформы разработки и используемых библиотек. Также описаны характеристики аппаратного обеспечения, на котором были выполнены дальнейшие эксперименты.

В разделе 3.2 представлена структура криптографического модуля в виде диаграмм классов и краткое описание функциональности ключевых компонентов.

В разделе 3.3 проведено экспериментальное исследование производительности защищенной и незащищенной доверенной цифровой подписи по сравнению с алгоритмом DSA, лежащим в основе доверенных модификаций. Сравнение времени выполнения приведено на рисунке 1.

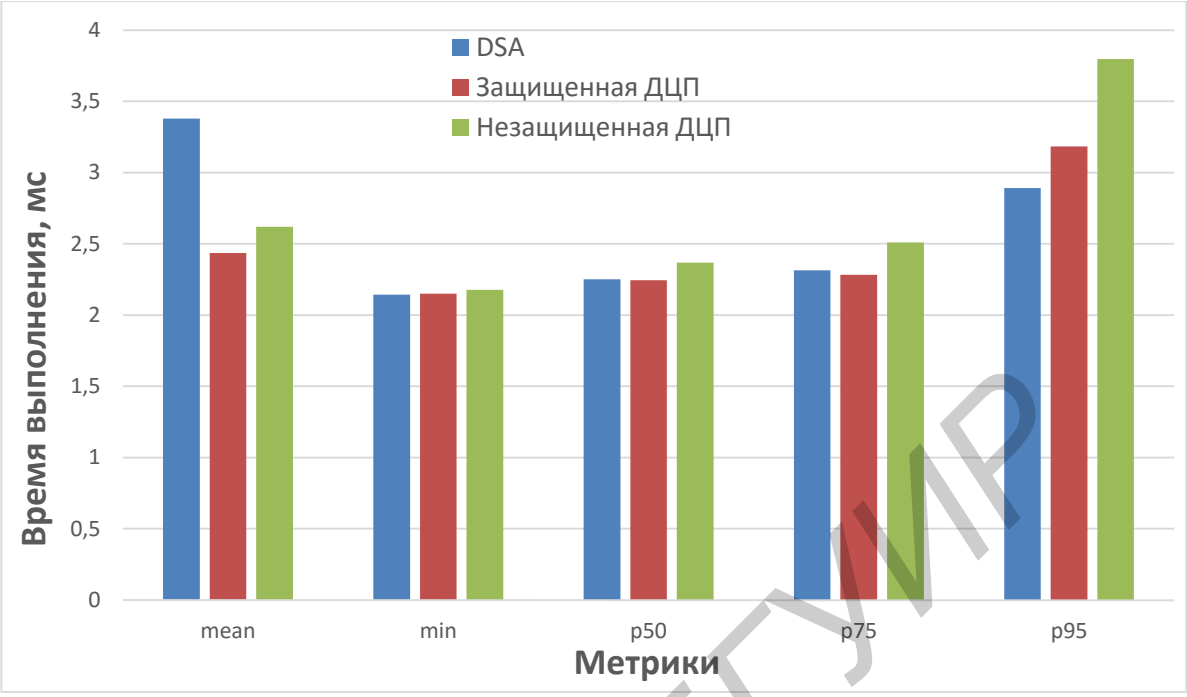

Рисунок 1 – Сравнение производительности модификаций ДЦП и базового алгоритма DSA

При анализе математической модели незащищенной и защищенной ДЦП в подразделах 2.4 и 2.5 был сделан вывод, что время, затраченное на процедуру подписания и верификации, не должно отличаться от исходного алгоритма цифровой подписи. В текущей реализации таким алгоритмом является DSA. Как видно по рисунку 1 все метрики практически не отличаются. Из этого можно заключить, что в данном случае теоретические положения выполняются. Также было проведено сравнение затрат на генерирование ключевой информации для защищенной и незащищенной модификаций. Результаты представлены на рисунке 2.

Таким образом на основании проведенных экспериментов можно убедиться, что производительность незащищенной и защищенной ДЦП зависит лишь от используемой схемы цифровой схемы, в данном случае DSA. Накладные расходы для генерации доверенности незначительные, которыми можно пренебречь. Поэтому можно сделать вывод, что дальнейшее развитие ДЦП может получить, заменив базовый алгоритм DSA на ECDSA, который базируется на эллиптических кривых. Данная модификация предоставит новый уровень безопасности и быстродействия.

В разделе 3.6 проведен детальный анализ производительности пороговой схемы доверенной цифровой подписи на различных этапах протокола и экспериментально показаны слабые места протокола, которые требуют доработки.

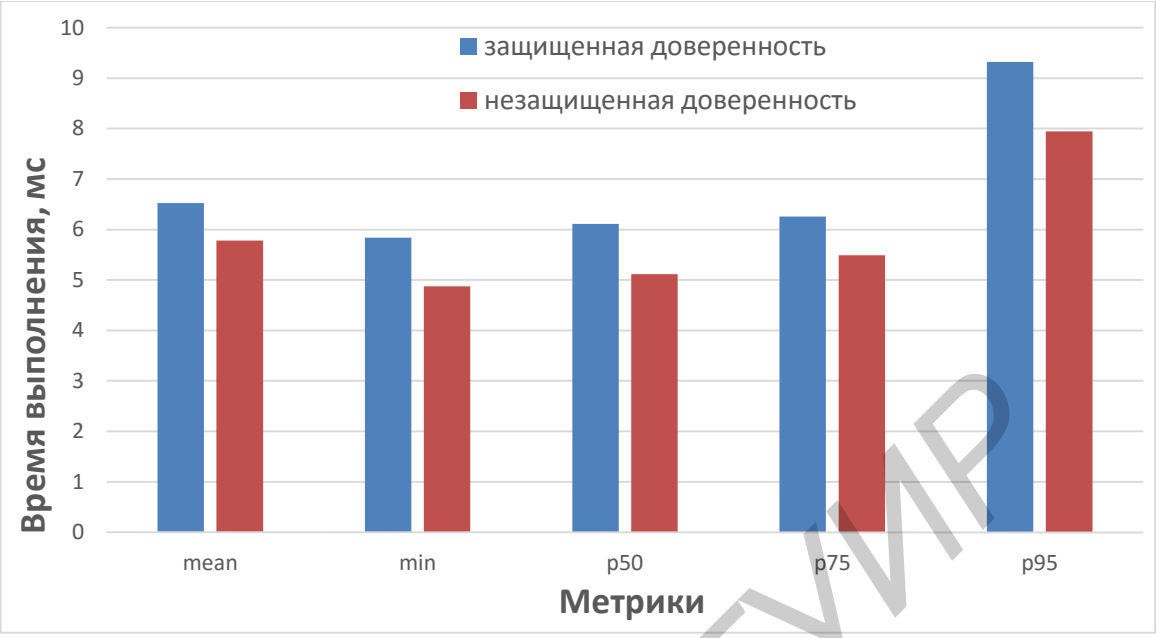

Рисунок 2 – Сравнение затрат на генерирование ключевой информации

Из проведенного эксперимента над пороговой доверенной цифровой подписью можно сделать вывод, что затраты для подписания документа сильно зависят от пороговой схемы, в которой происходит делегирование. Было показано, что делегирование полномочий на подписание группе масштабируется при увеличении порогового значения. Наиболее затратным является процесс генерации ключевой информации и частей подписи. Эти операции плохо масштабируются при увеличении порогового значения для группы и требуют улучшения. Тем не менее, если пороговая величина остаётся не очень большой (полученные экспериментальные данные говорят, что для порогового значения 7 временные затраты являются удовлетворительными), то даже для больших групп состоящих из десятка участников протокол Ceredo Schnorr [20] показывает неплохие результаты по временным затратам.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

В результате написания магистерской диссертацией разработан криптографический модуль, позволяющий ставить ЭЦП по алгоритму DSA, незащищенную доверенную цифровую подпись, защищенную доверенную цифровую подпись, а также предоставляет возможность генерации пороговой доверенной цифровой подписи в группе.

Используя разработанный криптографический модуль были проведены экспериментальные исследования, в рамках которых были показаны основные

метрики производительности протоколов, произведено сравнение с аналогами. Были показаны как дополнительные свойства доверенных протоколов влияют на общую производительность схемы, которая лежит в основе модификации.

В рамках магистерской диссертации были получены следующие результаты:

– рассмотрен математический аппарат, который лежит в основе криптографии с открытым ключом;

– описана и проанализирована общая схема протокола ДЦП;

– описана и проанализирована математическую модель протокола доверенной цифровой подписи частичного делегирования на основе криптосистемы ElGamal исходя из полученной ранее общей схемы доверенностью и выявить математический аппарат, который позволяет получить уникальные свойства данной модификации;

– определены, какие математические операции могут замедлить работу протокола незащищенной ДЦП;

– описана и проанализирована математическая модель протокола защищенной доверенной цифровой подписи частичного делегирования с доверенностью исходя из полученной ранее общей схемы доверенностью и выявлен математический аппарат, который позволяет получить уникальные свойства данной модификации;

– определены какие математические операции могут замедлить работу протокола защищенной ДЦП;

– описана и проанализирована математическая модель протокола пороговой доверенной цифровой подписи;

– определены шаги, которые в протоколе взаимодействия могут замедлить работу схемы пороговой ДЦП;

– программно реализованы протоколы на базе полученных математических моделей, которые помогут экспериментально проверить достоверность описанного математического аппарата;

– описана общую структура полученного криптографического модуля;

– проведены экспериментальная оценка сложности дополнительных вычислений в незащищенной и защищенной ДЦП;

– проанализированы незащищенная и защищенная ДЦП с алгоритмом DSA, лежащим в их основе;

– проанализированы данные о производительности схемы DSA с полученными реализациями.

Результаты проделанной работы в рамках магистерской диссертации были опубликованы на «51-ой научной конференции аспирантов, магистрантов и студентов БГУИР» по направлению компьютерные системы и сети [1-А], а также на конференции «Дистанционное обучение – образовательная среда XXI века» в секции 4 «Информационные компьютерные сети и системы в сфере образования» [2-А].

Рекомендации по практическому использованию результатов

1. Полученные результаты формируют отличную теоретическую базу для изучения механизмов работы модификаций доверенной цифровой подписи.

2. Разработанный криптографический модуль может служить основой для проведения экспериментальных исследований в области ДЦП, а также применяться как основа для построения программного обеспечения, которое нуждается в алгоритмах ДЦП.

3. Полученные экспериментальные данные могут послужить основой для дальнейших исследований в области ДЦП, намечены пути развития представленных алгоритмов.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Еленевич, Р.В. Защищенная схема доверенной цифровой подписи на основе криптосистем с открытым ключом / Р.В. Еленевич, В.Н. Ярмолик // 51-я научная конференция аспирантов, магистрантов и студентов по направлению 4: Компьютерные системы и сети: Тезисы докл. – Минск : БГУИР, 2015. – с. 66 - 67.

2-А. Еленевич, Р.В. Защищенная схема доверенной цифровой подписи с полномочиями в системах дистанционного / Р.В. Еленевич // Дистанционное обучение – образовательная среда XXI века. Секция 4: Информационные компьютерные сети и системы в сфере образования: Тезисы докл. – Минск : БГУИР, 2015. – с. 292 - 293.