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

УДК_____

Коминч
Вадим Витальевич

Стандарт цифровой подписи СТБ 34.101.45 на базе ПЛИС

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-40 80 01 «Компьютерная инженерия»

Научный руководитель
Станкевич Андрей Владимирович
доцент, кандидат технических наук

Минск 2021

ВВЕДЕНИЕ

Задача идентификации автора документа стала особенно остро с развитием информационных технологий. Использование для этих целей алгоритмов хеширования не дало значительных успехов.

Для этих целей были разработаны алгоритмы цифровой подписи. Они позволили добиться двух целей: удостовериться в подлинности авторства и обеспечить уникальность документа. Используемые для этого схемы разнообразны и используют различные математические задачи для генерации подписи: задача дискретного логарифмирования и задача факторизации больших чисел.

Наиболее широко используемая задача дискретного логарифмирования и вошла в состав многих стандартов подписей, в том числе и в белорусский стандарт. Невозможность решения задачи за приемлемое время позволило использовать задачу без боязни быть взломанным.

Реализованный программно алгоритм имеет значительно меньше путей для оптимизации решения. В то же время открытые аппаратные реализации и их анализ позволяют утверждать, что полученные схемные реализации устройств могут работать гораздо быстрее, чем их программные аналоги. Кроме того, их оптимизация может проводиться в нескольких направлениях, а полученные решения позволят ещё больше ускорить полученное устройство.

Основными задачами работы являются анализ алгоритмов цифровой подписи, схемы их генерации, а также реализация законченного устройства.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель данной работы: разработка оптимального с точки зрения производительности и аппаратных затрат устройства формирования цифровой подписи на базе ПЛИС.

Задачи исследования: анализ аппаратных реализаций стандартов различных стран, максимизация производительности, оптимизация расхода аппаратных ресурсов.

Объект исследования: электронная цифровая подпись, алгоритмы её генерации и архитектурные решения устройства для ее формирования.

Предмет исследования: аппаратные реализации стандартов цифровой подписи.

Личный вклад автора выражен в самостоятельном исследовании:

– анализ стандартов и алгоритмов цифровой подписи;

– сравнительный анализ существующих аппаратных реализаций устройств;

– анализ алгоритмов цифровой подписи с целью максимизации производительности и минимизации аппаратных затрат;

– исследование аппаратных затрат и производительности реализации стандарта цифровой подписи.

Результатом произведенного анализа, расчетов и оптимизации явилась разработка собственного устройства формирования цифровой подписи на основе белорусского стандарта.

Практическая значимость результатов диссертации состоит в разработке устройства для формирования цифровой подписи.

Материалы диссертации докладывались на 55-й и 56-й научной конференции аспирантов, магистрантов и студентов БГУИР.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В ведении показано, как происходило развитие систем безопасности для документов.

Использование только лишь алгоритмов шифрования и хеширования не позволило обеспечить надлежащий уровень защиты, а с развитием вычислительной мощности компьютеров задача взлома стала достижимой за приемлемое время.

Использование алгоритмов электронной цифровой подписи позволило решить проблему авторства данных и их уникальности.

Выделены основные задачи работы:

1. Провести анализ известных алгоритмов цифровой подписи и их аппаратных реализаций.
2. Провести анализ алгоритмов стандарта СТБ.34.101.45 – 2013 с точки зрения особенностей их реализаций на базе ПЛИС с целью минимизации аппаратных затрат и максимизации производительности.
3. Выбрать архитектуру и реализовать на базе ПЛИС специализированный процессор цифровой подписи в соответствии со стандартом СТБ.34.101.45 – 2013.
4. Исследовать аппаратные затраты и производительность разработанного специализированного процессора.

В главе 1 проведён сравнительный анализ алгоритмов электронной цифровой подписи Украины, России, США и Беларуси. Рассмотрены эллиптические кривые, выполнение основных операций над точками кривых в конечном поле. Проанализированы кривые различных характеристик. Кроме того рассмотрены алгоритмы хеширования, используемые в каждом стандарте, проанализированы схемы генерации подписи. Введены понятия вычислений в конечном поле, проведён вывод формул для алгебраического вычисления координат точек эллиптической кривой.

Рассмотрены некоторые алгоритмы умножения и деления по модулю как наиболее часто встречающиеся в алгоритме вычисления k-кратной точки.

Далее приводятся различные аппаратные реализации американского стандарта подписи. Показаны основные отличия в реализации, проведён сравнительный анализ используемых архитектур, рассмотрены достоинства и недостатки каждой из архитектур. В основе каждого устройства лежит идея использования архитектуры процессора общего назначения. Для работы устройств вычисление подписи должно быть закодировано с помощью машинных команд и сохранено в памяти. Так как алгоритм подписи не подразумевает огромного числа вычислений, то использование системы команд в устройствах не оправдано. Также стоит отметить, что рассматриваемые устройства являются уни-

версальными, не заточенными только лишь под вычисление цифровой подписи. Часть архитектур использовала для вычисления декартовы координаты, которые требовали использования деления в каждом такте работы процессора.

Во второй главе проводится анализ белорусских алгоритмов с целью их аппаратной реализации. Проведена оценка сложности алгоритмов цифровой подписи. Алгоритмы хеширования и шифрования блока имеют вычислительную сложность O(N), что позволило провести некоторые оптимизации при проектировании архитектуры данных блоков. Для сравнения расхода ресурсов и времени выполнения были реализованы два архитектурных решения блока шифрования.

Первый блок, для которого необходимо проводить оптимизацию, является блок вычисления k-кратной точки. Занимающий более 90% вычислительного времени он является критически важным при ускорении проекта.

В качестве одного из инструментов оптимизации были использованы различные координатные системы: проективная и система Якоби. Рассмотрен перевод координат из декартовой системы в обе системы. Проанализирован вычислительный процесс при использовании каждой координатной системы. Использование трёхмерных координатных систем хотя и увеличивает количество операций в схеме, однако позволяет отказаться от вычисления деления в вычислении итерации работы блока. Деление появляется только при переводе координат.

Были проанализированы методы вычисления k-кратной точки с целью максимизации производительности. Выбранный алгоритм вычисления алгоритм Монтгомери позволил использовать блоки сложения точек и удвоения точки параллельно.

Блок хеширования был оптимизирован с помощью оптимизации внутреннего блока шифрования. Для более производительного решения цепочки сумматоров и вычитателей были разбиты с помощью регистров. Это позволило проводить вычисления в разных тактах и ускорить тактовую частоту.

В главе 3 представлена разработанное устройство цифровой подписи. Для его создания были проанализированы различные архитектурные решения, позволяющие добиться одной из целей: увеличение производительности или уменьшение расхода ресурсов.

Отдельно рассмотрена реализация основных функциональных узлов: хеширования, вычисления k-кратной точки.

При реализации хеширования были использованы предложенные ранее улучшения архитектуры. В частности использование регистров для разбиения цепочек сумматоров в алгоритме шифрования, использования сдвоенного блока вычисления внутренних сигналов в блоке хеширования.

Для блока вычисления k-кратной точки была показана выбранная архитектура. Были рассмотрены диаграммы вычислительного процесса блоков сложения точек и удвоения точки.

Также были показаны основные этапы разработки всего устройства, включая :

– Выбор различных архитектурных решений и его аргументация;
– Структурные схемы блоков и граф-схемы состояний;
– Временные диаграммы блоков.
– Расход аппаратных ресурсов.

Структурная схема полученного устройства представлена на рисунке 1.

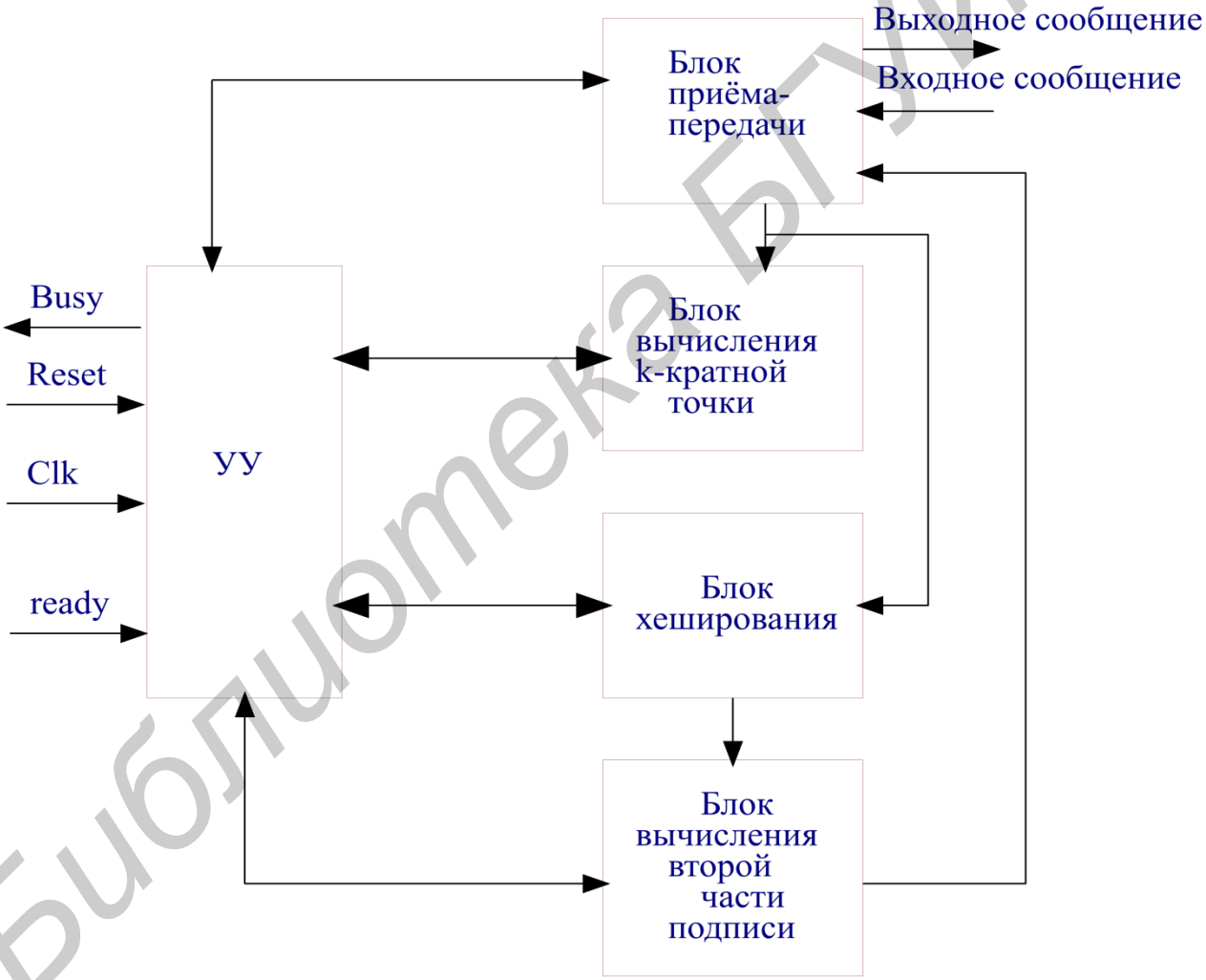

Рисунок 1 – Структурная схема полученного устройства

В качестве функции хеширования выступает алгоритм, определённый в стандарте СТБ 34.101.31 – 2011 , что и алгоритм шифрования блока. Для данного алгоритма длина входного сообщения не ограничена сверху. Используемые внутри него операции позволяют быстро вычислять хеш-значение входного со-

общения. Важной особенностью алгоритмов хеширования является дополнение входного сообщения в случаях, если его длина не кратна размеру блока хеширования. Существует несколько схем дополнения, самой простой из которых является дополнение нулями остатка. Такая схема используется в алгоритме из белорусского стандарта.

Алгоритм хеширования, как и алгоритм шифрования, предполагает однократный проход по входным данным. Данный факт позволяет оценить сложность алгоритма также как O(N). Однако в отличие от алгоритма шифрования количество итераций блока хеширования явно зависит от длины входного сообщения, что накладывает некоторые трудности при дальнейшей реализации.

Одним из самых важных блоков в устройстве является блок вычисления k-кратной точки. Вычисления произведения сводится к вычислению суммы точек. Для ускорения вычислений могут быть использованы алгоритмы, такие как умножение Монтгомери, также возможно использование различных координатных систем для уменьшения количества делений в схеме.

Основные используемые координатные системы, которые разумно применять при вычислениях, основаны на добавлении третьей координаты. Постепенно заменяя все операции через операции с тремя переменными операции деления вырождаются.

В таблицах 1 и 2 приведены используемые операции при вычислении операций удвоения и сложения над точками эллиптической кривой. Как видно из таблиц замена системы координат позволяет убрать операцию деления из вычислений.

Таблица 1 – Сравнение вычислительной сложности удвоения точки

Система координат	сложение	умножение	деление
Декартовы координаты	6	4	1
Проективные координаты	3	7	0

Таблица 2 – Сравнение вычислительной сложности сложения точек

Система координат	сложение	умножение	деление
Декартовы координаты	6	2	1
Проективные координаты	2	12	0

Тестирование устройства проводилось согласно выделенных в работе логических уровней. Тестовые примеры для блока шифрования, хеширования, цифровой подписи были взяты из соответствующих стандартов.

Для проверки работоспособности блока вычисления k-кратной точки была разработана программа на языке программирования Python, с результатами которой и сверялись результаты работы блока.

Временные диаграммы устройства представлены на рисунках 2-5.

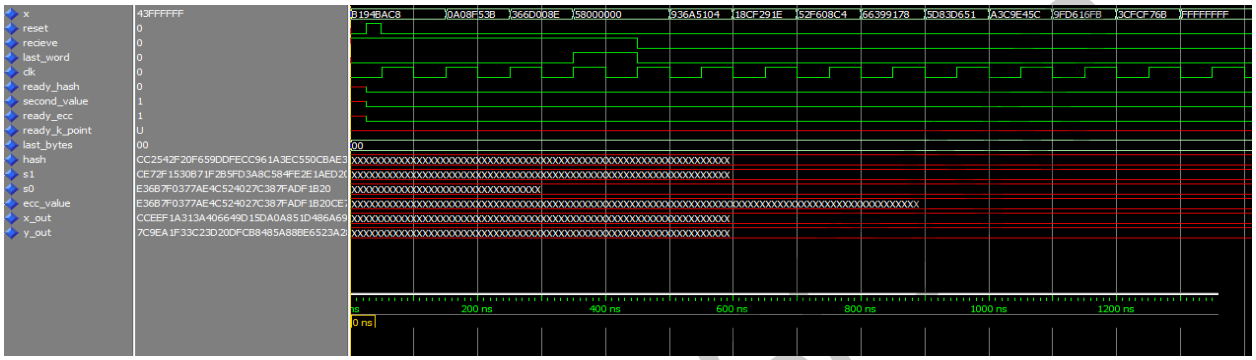

Рисунок 2 – Временная диаграмма начала работы устройства цифровой подписи

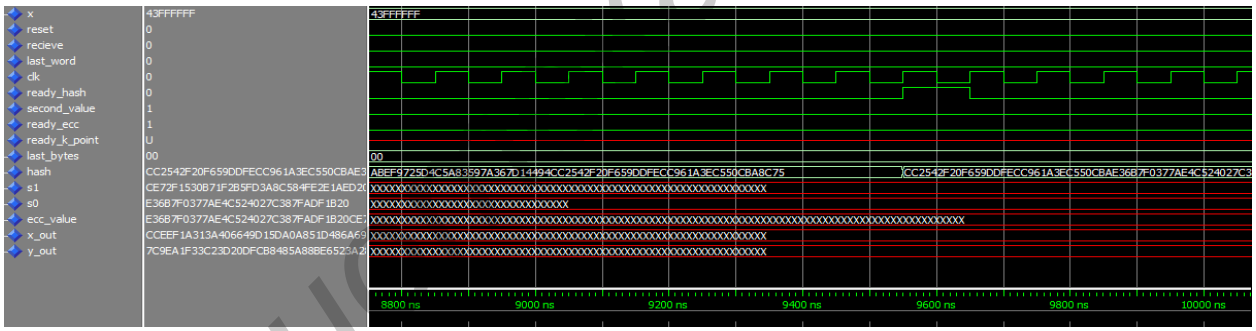

Рисунок 3 – Временная диаграмма работы блока хеширования в устройстве

Аналогично проверялся блок вычисления кратной точки. Результат работы блока сверялся с тестовыми данными и значениями блоков из стандарта.

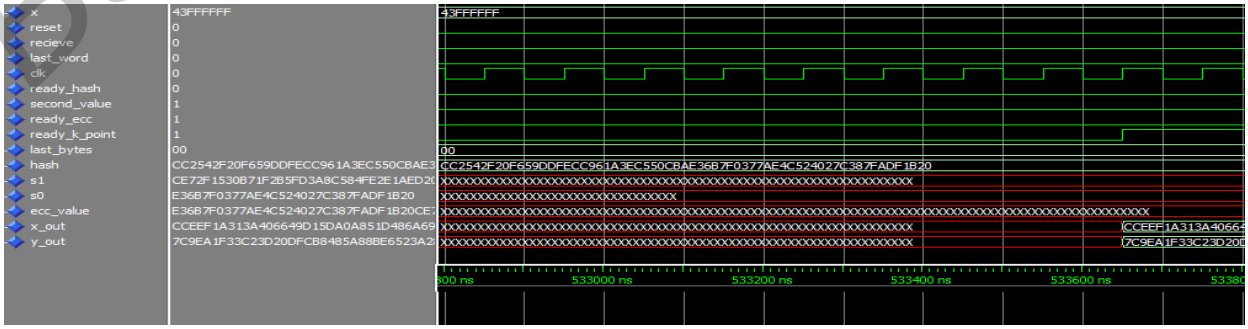

Рисунок 4 – Временная диаграмма работы блока вычисления k-кратной точки

Последние вычисления в устройстве связаны с вычислением второй части подписи. Результат вычислений, а также окончание работы устройства представлены на рисунке 3.26.

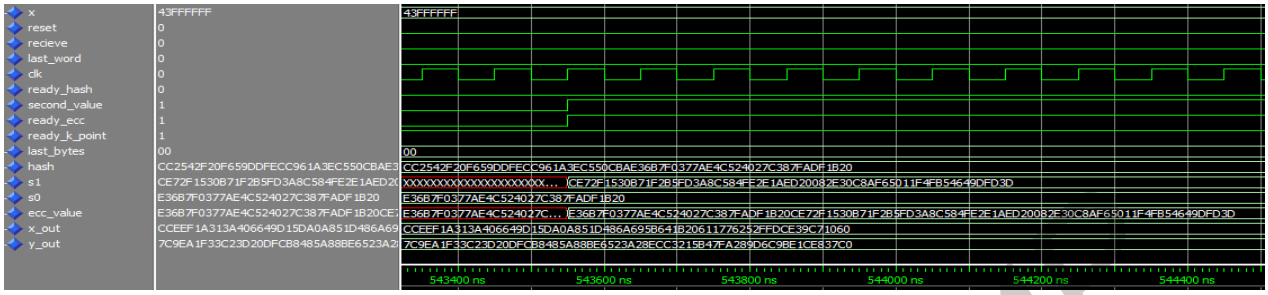

Рисунок 3.26 – Временная диаграмма окончания работы устройства

Был разработан дополнительный функциональный блок – блок приёма сообщения. Он позволил обрабатывать сообщения, чья длина превышает максимальное количество портов ПЛИС.

Для кристалла ПЛИС xc7v585t семейства Xilinx Virtex 7 полученная после процедуры синтеза тактовая частота составляет 151,7МГц. Время вычисления цифровой подписи – 543,6 мкс. Полученные результаты свидетельствуют о выполнении цели и задач исследования.

Для оценки площади занимаемого проекта была проведена операция синтеза. Полученные результаты говорят о том, что вычислительный процесс устройства может быть дополнительно ускорен за счёт параллельного размещения большего числа вычислительных блоков.

ЗАКЛЮЧЕНИЕ

Результатом проведенного исследования стала разработка полноценного устройства цифровой подписи. В ходе работы были рассмотрены различные алгоритмы цифровой подписи, принятые в качестве национальных стандартов, основные алгоритмы, входящие в состав цифровой подписи белорусского стандарта.

В работе были рассмотрены алгоритмы цифровой подписи различных стран в сравнении с белорусским стандартом. Были проанализированы аппаратные реализации соответствующих стандартов. Проведен анализ алгоритмов стандарта СТБ.34.101.45 – 2013 с точки зрения особенностей их реализаций на базе ПЛИС с целью минимизации аппаратных затрат и максимизации производительности. На основе проведенного анализа была выбрана смешанная итерационно-конвейерная архитектура специализированного процессора с использованием распараллеливания вычислений при выполнении операций удвоения и сложения точки.

Архитектура устройства описана с помощью языка VHDL и синтезирована средствами САПР ISE 14.7. Для подтверждения работоспособности было проведено тестирование полученного устройства на тестовых примерах из стандарта СТБ 34.101.45 – 2013.

Для кристалла ПЛИС xc7v585t семейства Xilinx Virtex 7 полученная после процедуры синтеза тактовая частота составляет 151,7МГц. Время вычисления цифровой подписи – 543,6 мкс. Полученные результаты свидетельствуют о выполнении цели и задач исследования.

Разработанный процессор может использоваться как IP-ядро для генерации цифровой подписи документов.

Предложены некоторые направления дальнейшего улучшения архитектуры устройства. Среди них поиск оптимальных координатных систем, которые позволят вычислять результат сложения и удвоения без огромного количества операций умножения по модулю. Кроме того, исследования могут проводиться и для нахождения оптимального способы нахождения инверсии по модулю, так как данная операция в любом случае используется при работе устройства.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1-А.] Коминч В.В. Эллиптические кривые в электронной цифровой подписи. // В.В.Коминч. // 56-я научная конференция аспирантов, магистрантов и студентов БГУИР.

[2-А.] Коминч В.В. Электронная цифровая подпись на базе эллиптических кривых. // В.В.Коминч. // 55-я юбилейная научная конференция аспирантов, магистрантов и студентов БГУИР.