Yerbol Amangazovich Ospanov* – PhD, Associate Professor, Shakarim University, Semey, Republic of Kazakhstan; e-mail: y.ospanov@shakarim.kz. ORCID: https://orcid.org/0000-0001-5342-274X.

Редакцияға енуі 30.03.2026
Өңдеуден кейін түсуі 16.04.2026
Жариялауға қабылданды 17.04.2026

https://doi.org/10.53360/2788-7995-2026-2(22)-2

МРНТИ: 47.14.07, 81.93.29

И.А. Сенюшин[1], Н.С. Глазырина[1]*, Р.Б. Ибраев[1], Е.К. Джилкибаев[1], А. Әділғазыұлы[2]
[1]ТОО «TSARKA R&D»,
010000, Республика Казахстан, г. Астана, проспект Кабанбай Батыра, 51/1
[2]Назарбаев Университет,
010000, Республика Казахстан, г. Астана, проспект Кабанбай Батыра, 53
*e-mail: glazirinan@yandex.ru

ФОРМАЛИЗОВАННЫЙ МАРШРУТ РАЗРАБОТКИ КРИПТОГРАФИЧЕСКОГО КОНТРОЛЛЕРА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ С ПЛИС-ВЕРИФИКАЦИЕЙ

Аннотация: *В статье представлен и экспериментально апробирован формализованный маршрут разработки специализированного криптографического контроллера для аппаратной реализации алгоритмов электронной цифровой подписи. Разработанный маршрут охватывает полный цикл проектирования и включает этапы архитектурного синтеза, RTL-реализации, аппаратной верификации на ПЛИС и физической реализации в рамках MPW-потока. Архитектура контроллера построена по модульному принципу, при котором система представляет собой совокупность функционально независимых аппаратных блоков, разрабатываемых и верифицируемых как отдельные модули. Для каждого блока выполняются RTL-реализация, формирование программного интерфейса и аппаратная верификация на этапе ПЛИС-прототипирования, что обеспечивает раннее выявление функциональных и интерфейсных ошибок. Для критически важных компонентов дополнительно применяется физическая верификация в маршруте RTL-to-GDS с прохождением проектных проверок, включая DRC и LVS. После завершения модульной верификации выполняется интеграция блоков, формируется карта памяти и проводится системная аппаратная верификация. Экспериментальная апробация выполнена на демонстрационном вычислительном модуле на базе ядра TinyQV (RISC-V) с использованием платформ GOWIN Tang Primer 20K и TinyTapeout (PDK SkyWater SKY130). Полученные результаты подтверждают воспроизводимость предложенного маршрута и его практическую применимость для разработки специализированных криптографических контроллеров и защищённых встраиваемых систем.*

Ключевые слова: *криптографический контроллер, электронная цифровая подпись, ПЛИС прототипирование, аппаратная верификация, MPW прототипирование, информационная безопасность.*

Введение

В современных государственных, финансовых и корпоративных информационных системах одной из ключевых задач является обеспечение защищённого электронного документооборота и выполнения электронных транзакций. Для решения данной задачи широко применяется электронная цифровая подпись (ЭЦП), обеспечивающая подлинность источника, целостность данных и неотказуемость авторства электронных документов [1-4]. В отличие от программной реализации, аппаратная реализация ЭЦП на базе специализированных криптографических контроллеров обеспечивает более высокий уровень защищённости за счёт изоляции ключевого материала и снижения зависимости от уязвимостей программного обеспечения [5-9].

В научной литературе широко представлены исследования, посвящённые аппаратной реализации алгоритмов электронной цифровой подписи, включая ускорители RSA, решения на эллиптических кривых (ECDSA, EdDSA), а также реализации алгоритмов ГОСТ [10-17]. Одновременно развиваются подходы к верификации систем-на-кристалле (SoC), включая функциональную и формальную верификацию, FPGA-прототипирование и open-source маршруты физического проектирования ASIC [18-27].

Несмотря на значительное количество исследований, посвящённых отдельным аспектам аппаратной реализации криптографических алгоритмов и проектирования SoC, в научной литературе недостаточно представлены формализованные и воспроизводимые маршруты разработки криптографических контроллеров, охватывающие полный цикл от архитектурного проектирования до физической реализации [28-32]. Отсутствие такого сквозного подхода приводит к выявлению архитектурных и интерфейсных ошибок на поздних стадиях разработки и увеличивает технологические риски.

Работа выполнена в рамках проекта AP26103891 «Разработка отечественного криптоконтроллера и его имплементация в устройстве хранения ключей». Разрабатываемый криптографический контроллер ориентирован на применение в составе защищённых устройств хранения ключевой информации и средств аппаратной аутентификации, поддерживающих алгоритмы ЭЦП и стандарт FIDO [33, 34].

Целью работы является разработка и экспериментальная апробация формализованного маршрута разработки специализированного криптографического контроллера для алгоритмов электронной цифровой подписи, основанного на поэтапной FPGA-верификации и физической апробации функциональных модулей и интегрированной системы.

Научная новизна работы заключается в разработке формализованного и воспроизводимого маршрута проектирования специализированного криптографического контроллера, отличающегося интеграцией модульной FPGA-верификации, выборочной физической апробации критически важных компонентов в маршруте RTL-to-GDS и системной верификации интегрированной архитектуры до этапа MPW-прототипирования. В отличие от существующих подходов, ориентированных на реализацию отдельных криптографических ускорителей или отдельных этапов верификации, предложенный маршрут обеспечивает сквозной процесс разработки, позволяющий выявлять архитектурные и интерфейсные ошибки на ранних стадиях и снижать риски физической реализации.

Условия и методы исследования

В рамках настоящей работы предлагается формализованный маршрут разработки специализированного криптографического контроллера, представляющий собой последовательность взаимосвязанных этапов проектирования и верификации, обеспечивающих воспроизводимость процесса разработки и снижение технологических рисков. Предложенный подход основан на модульном принципе построения системы и поэтапной аппаратной и физической апробации функциональных блоков.

Первый этап включает архитектурное проектирование криптографического контроллера с определением структуры системы и состава функциональных модулей, включая вычислительные, системные и специализированные криптографические блоки.

Второй этап предполагает модульную разработку, при которой каждый функциональный блок реализуется на уровне RTL и проходит функциональную верификацию. Параллельно формируется слой аппаратной абстракции (Hardware Abstraction Layer, HAL), обеспечивающий программный интерфейс к аппаратным компонентам.

Далее выполняется аппаратная верификация модулей на ПЛИС, позволяющая подтвердить корректность их функционирования в условиях реальной аппаратной среды.

Для физической апробации критически важных модулей применяется MPW-подход с использованием автоматизированного маршрута RTL-to-GDS, включающего логический синтез, размещение, трассировку и выполнение проектных проверок (DRC, LVS), что позволяет подтвердить корректность физической реализации.

После завершения модульной апробации осуществляется поэтапная интеграция функциональных блоков в состав единой архитектуры, формируется карта памяти системы и выполняется финализация HAL.

Интегрированная архитектура проходит системную аппаратную верификацию на ПЛИС, включающую проверку межмодульного взаимодействия и корректности выполнения встроенного программного обеспечения.

На заключительном этапе интегрированная система реализуется в маршруте RTL-to-GDS и передаётся в MPW-шаттл для изготовления опытного образца интегральной схемы.

Общий маршрут разработки криптографического контроллера в рамках предлагаемого подхода представлен на рисунке 1. Подписи функциональных блоков на рисунках приведены на английском языке в соответствии с общепринятой терминологией, используемой в современных EDA-инструментах, языках аппаратного описания (Verilog, VHDL) и проектной документации. Это обеспечивает однозначное соответствие между схемами, RTL-описанием и аппаратной реализацией.

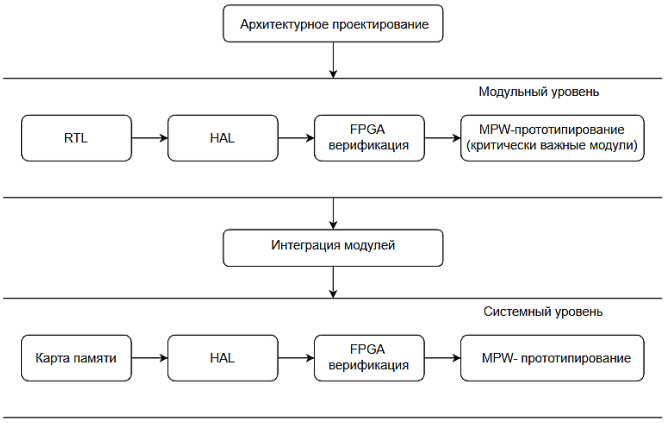

Рисунок 1 – Формализованный маршрут разработки криптографического контроллера с поэтапной аппаратной и физической верификацией

Представленный маршрут отражает последовательность этапов проектирования и верификации, обеспечивающую раннее выявление функциональных и интерфейсных ошибок, а также воспроизводимость процесса разработки при переходе от архитектурного уровня к физической реализации.

Для реализации физической апробации используется MPW-подход, обеспечивающий получение опытных образцов интегральных схем при существенно меньших затратах и сроках по сравнению с индивидуальным ASIC-производством. Применение MPW-подхода требует выбора платформы, обеспечивающей воспроизводимый маршрут проектирования, наличие открытого PDK и автоматизированного инструментального потока.

С этой целью выполнен сравнительный анализ доступных MPW-платформ с учётом технологического процесса, степени открытости инструментальной среды и уровня автоматизации проектирования (табл. 1).

Таблица 1 – Сравнение платформ MPW-прототипирования по технологическим и инструментальным характеристикам

Платформа	Процесс	Стоимость участия	PDK (SkyWater)	Автоматизированный процесс проектирования
GlobalFoundries MPW [35]	GF130, GF180, 65 nm, 22 nm	По запросу	No	Нет
MOSIS [36]	SkyWater SKY130, TSMC, GF, OnSemi	~10 000-12 000 USD	Ограничено	Нет
Muse Semiconductor [37]	TSMC 180 nm, 65 nm	1 250-14 000 USD	Нет	Нет
Cadence MPW (SkyWater) [38]	SkyWater SKY130	~10 000-12 000 USD	Нет	Нет
TinyTapeout [39]	SkyWater SKY130	~385 €	Да	Да

По результатам анализа установлено, что платформа TinyTapeout обеспечивает поддержку open-source PDK SkyWater SKY130, автоматизированный маршрут проектирования и открытую доступность, что обусловило её использование в рамках предлагаемого подхода.

Предложенный маршрут разработки позволяет обеспечить раннее выявление функциональных и интерфейсных ошибок, повысить воспроизводимость процесса проектирования и снизить риски, связанные с переходом к физической реализации.

Результаты исследований

Архитектура специализированного криптографического контроллера разработана на основе модульного принципа и включает вычислительное ядро, системную шину, подсистему памяти, периферийные интерфейсы и специализированные криптографические блоки (рис. 2).

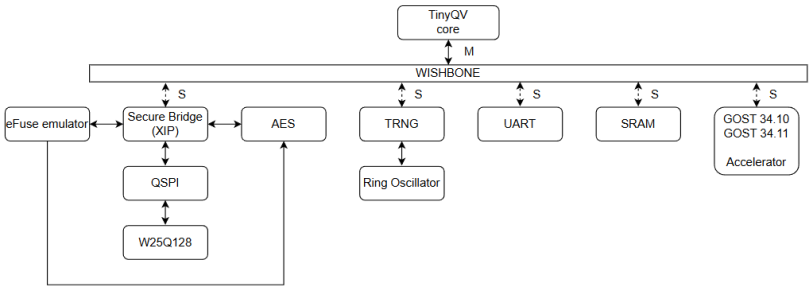

Рисунок 2 – Архитектура специализированного криптографического контроллера

Представленная архитектура отражает модульный подход к построению криптографического контроллера, обеспечивающий независимую разработку и верификацию функциональных блоков, а также их поэтапную интеграцию в составе системы. Такая организация позволяет снизить сложность проектирования, повысить управляемость процесса разработки и обеспечить согласованность интерфейсов при переходе к системной реализации.

В качестве демонстрационного модуля использован вычислительный модуль на базе процессорного ядра TinyQV (RISC-V), включающий основные функциональные компоненты процессорной архитектуры и подсистему доступа к памяти (рис. 3).

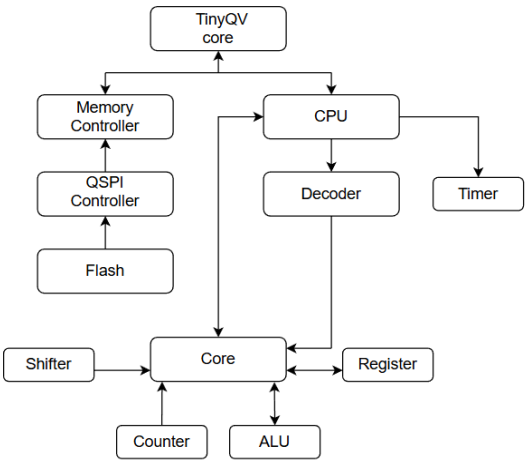

Рисунок 3 – Архитектура демонстрационного вычислительного модуля TinyQV

Демонстрационный модуль иллюстрирует базовую вычислительную подсистему, используемую для экспериментальной апробации предложенного маршрута разработки. Его применение позволяет подтвердить корректность функционирования ключевых компонентов архитектуры в реальной аппаратной среде и оценить применимость модульного подхода при переходе от RTL-описания к аппаратной реализации.

RTL-реализация вычислительного модуля выполнена на языке Verilog HDL. Иерархия RTL-модулей вычислительного ядра представлена на рисунке 4.

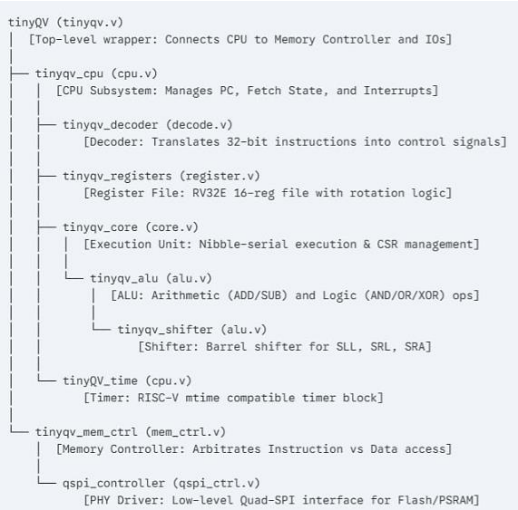

Рисунок 4 – Иерархия RTL-модулей вычислительного ядра TinyQV

Представленная иерархия RTL-модулей отражает структурную организацию вычислительного ядра, обеспечивающую разделение функциональности на уровни абстракции и модульную декомпозицию. Такая структура способствует упрощению верификации отдельных компонентов и повышает масштабируемость архитектуры при интеграции в состав криптографического контроллера.

Аппаратная верификация вычислительного модуля, совместимого с архитектурой RISC-V, выполнена на ПЛИС-платформе GOWIN Tang Primer 20K. В составе FPGA-проекта подсистема памяти реализована на основе примитивов BRAM ПЛИС Gowin в режиме Single Port. Для организации доступа к памяти использован модуль sim_qspi.v, обеспечивающий взаимодействие вычислительного ядра с подсистемой памяти.

Структурная схема взаимодействия вычислительного ядра с подсистемой памяти представлена на рисунке 5.

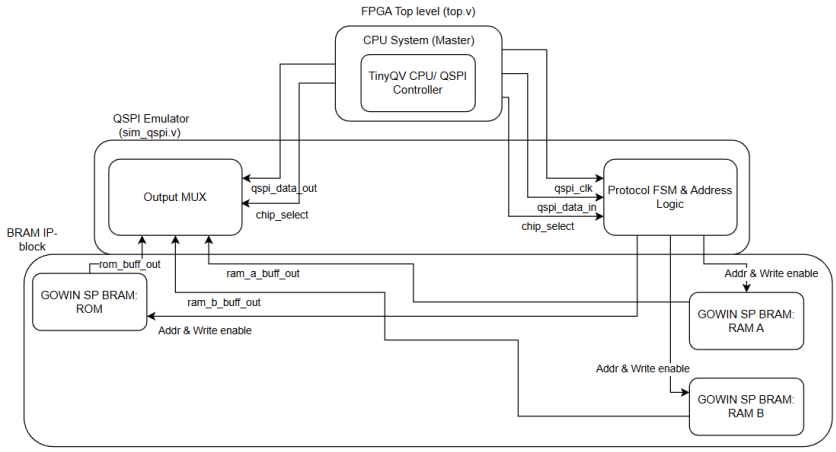

Рисунок 5 – Структурная схема взаимодействия вычислительного ядра TinyQV с подсистемой памяти в процессе FPGA-верификации

Данная схема демонстрирует организацию взаимодействия вычислительного ядра с подсистемой памяти в процессе аппаратной верификации и позволяет оценить корректность обмена данными между компонентами системы, а также согласованность интерфейсов при работе в реальной аппаратной среде.

В ходе ПЛИС-верификации подтверждена корректность функционирования подсистемы памяти, включая операции чтения и записи, адресацию и отсутствие конфликтов доступа. Дополнительно подтверждена корректность выполнения инструкций вычислительным ядром и устойчивость работы арифметико-логического устройства и механизма обратной записи.

Сопоставление результатов аппаратной реализации с данными RTL-моделирования показало отсутствие функциональных отклонений. Контроль аппаратного поведения системы осуществлялся с использованием встроенного логического анализатора, что позволило подтвердить корректность временных характеристик и стабильность работы вычислительного ядра при реализации на ПЛИС.

В ходе экспериментальной реализации получены количественные характеристики демонстрационного вычислительного модуля. Реализация на ПЛИС занимает порядка 2460 логических элементов (LUT) и 964 регистров (FF), при рабочей частоте до 27 МГц. Полученные значения подтверждают возможность реализации предложенной архитектуры в условиях ограниченных ресурсов ПЛИС и её пригодность для прототипирования.

Физическая реализация проекта выполнена с использованием автоматизированного маршрута OpenLane, включающего этапы логического синтеза, размещения и трассировки стандартных ячеек с последующей генерацией GDSII-файла. Подтверждено успешное прохождение проверок DRC и LVS, а также соответствие временных характеристик проекта заданным ограничениям.

При подготовке к MPW-прототипированию выполнена адаптация проекта к ограничениям платформы TinyTapeout, включая площадь размещения (конфигурация 3×2 тайлов), количество линий ввода-вывода (8 входных, 8 выходных и 8 двунаправленных), а также ограничение рабочей частоты до 64 МГц. По результатам прохождения автоматизированного маршрута проект передан в MPW-шаттл для изготовления опытного образца.

Предложенный маршрут разработки был применён не только к демонстрационному вычислительному модулю, но и к другим функциональным блокам криптографического контроллера, включая специализированные криптографические модули, реализующие алгоритмы электронной цифровой подписи. В рамках экспериментальной апробации выполнена интеграция функциональных блоков, сформирована карта памяти системы и проведена системная аппаратная верификация на ПЛИС, подтвердившая корректность межмодульного взаимодействия, функционирования подсистем памяти и периферийных интерфейсов, а также выполнения встроенного программного обеспечения.

Таким образом, полученные результаты подтверждают корректность предложенного формализованного маршрута разработки, его воспроизводимость и применимость для проектирования специализированных криптографических контроллеров и защищённых SoC-решений.

Обсуждение научных результатов

Полученные экспериментальные результаты позволяют перейти к анализу эффективности предложенного формализованного маршрута разработки специализированного криптографического контроллера.

Ключевым результатом проведённой экспериментальной апробации является подтверждение эффективности модульного подхода, при котором корректность архитектурных решений и согласованность интерфейсов проверяются на уровне отдельных функциональных блоков до их интеграции. Такой подход позволяет выявлять потенциальные архитектурные и интерфейсные несоответствия на ранних стадиях проектирования и тем самым снижать риски, связанные с переходом к физической реализации.

Экспериментальная апробация предложенного маршрута на демонстрационном вычислительном модуле TinyQV показала корректность выполнения инструкций, функционирования подсистемы памяти и стабильность работы вычислительного ядра в реальной аппаратной среде. Полученные количественные характеристики реализации на ПЛИС (2460 логических элементов (LUT), 964 регистров (FF), рабочая частота до 27 МГц) подтверждают возможность реализации предложенной архитектуры в условиях ограниченных аппаратных ресурсов и её применимость для прототипирования.

Важным результатом является подтверждение применимости данного подхода к переходу от RTL-описания к физической реализации. Успешное прохождение автоматизированного маршрута OpenLane демонстрирует технологическую корректность и воспроизводимость разработки в open-source инструментальном потоке.

Для сопоставления предложенного подхода с существующими исследованиями выполнен сравнительный анализ по ключевым характеристикам маршрута разработки (табл. 2).

Таблица 2 – Сравнение предложенного подхода с существующими работами

Подход / работа	FPGA-верификация	RTL-to-GDS	Сквозной маршрут разработки	Воспроизводимость
Работы [13-15]	Да	Нет	Нет	Нет
Работы [25-27]	Нет	Да	Частично	Да
Предлагаемый подход	Да	Да	Да	Да

Как следует из таблицы, существующие исследования, как правило, ориентированы либо на реализацию отдельных криптографических модулей, либо на отдельные этапы проектирования и верификации. В отличие от них, предложенный подход обеспечивает сквозной воспроизводимый маршрут разработки, объединяющий архитектурное проектирование, модульную FPGA-верификацию, выборочную физическую апробацию и системную интеграцию.

Помимо демонстрационного вычислительного модуля, данный маршрут применяется также к специализированным криптографическим блокам. Дополнительную значимость представляют их количественные оценки. В частности, для аппаратных ускорителей алгоритмов электронной цифровой подписи (СТ РК ГОСТ Р 34.10-2015) получены предварительные ресурсные характеристики порядка 14602 логических элементов (LUT), 6702 регистров (FF), рабочая частота до 23,9 МГц, что подтверждает возможность реализации таких модулей в рамках разработанного маршрута.

Следует отметить, что в рамках настоящего исследования основной акцент сделан на формализации маршрута разработки и его экспериментальной апробации. Полученные количественные оценки демонстрируют перспективность данного подхода и формируют основу для дальнейшей оптимизации криптографических модулей по показателям производительности, площади и энергопотребления.

В целом результаты исследования показывают, что разработанный маршрут обеспечивает воспроизводимый переход от архитектурного проектирования к аппаратной и физической реализации и может рассматриваться как практическая основа для создания специализированных криптографических контроллеров и защищённых систем-на-кристалле.

Заключение

В работе представлен и экспериментально апробирован формализованный маршрут разработки специализированного криптографического контроллера для аппаратной реализации алгоритмов электронной цифровой подписи.

Предложенный подход основан на модульном принципе и предусматривает поэтапную проверку корректности отдельных функциональных блоков с последующей интеграцией и системной верификацией. Экспериментальная апробация на демонстрационном вычислительном модуле TinyQV продемонстрировала корректность функционирования архитектуры на уровне RTL и ПЛИС, а также возможность перехода к физической реализации с прохождением проверок DRC и LVS.

Полученные количественные характеристики реализации (2460 логических элементов (LUT), 964 регистров (FF), рабочая частота до 27 МГц) подтверждают применимость данного подхода в условиях ограниченных аппаратных ресурсов и его пригодность для прототипирования специализированных криптографических устройств.

Результаты исследования показывают, что разработанный маршрут обеспечивает воспроизводимый процесс разработки и может быть использован при создании специализированных криптографических контроллеров и защищённых систем-на-кристалле.

Перспективы дальнейших исследований связаны с расширенной оценкой специализированных криптографических модулей по показателям производительности, площади и энергопотребления, а также анализом устойчивости аппаратной реализации к атакам по побочным каналам.

Список литературы

1. Meng H. Research and development of digital signatures / Meng H., Sang Z. // Journal of Computing and Electronic Information Management. – 2025. – Vol. 16, № 3. – P. 23-28.
2. Gashi K. Digital signatures in the modern era: a review of cryptographic progress and post-quantum challenges / K. Gashi, B. Hyseni // International Journal of Innovative Technology and Interdisciplinary Sciences. – 2025. – Vol. 8, № 4. – P. 1082-1112.
3. Trends in data protection and encryption technologies / V. Mulder et al. – Switzerland: Springer, 2023. – 225 p.
4. Somsuk K. The development of signing and verification methods for high speed digital signatures on electronic official documents by using RSA cryptography / K. Somsuk // Cogent Engineering. – 2024. – Vol. 11, № 1. – Art. 2432513. https://doi.org/10.1080/23311916.2024.2432513.
5. Implementation efficiency of Falcon digital signature scheme on Arty-7 XC7A35T board / T.-T. Nguyen et al // Electronics. – 2025. – Vol. 14, № 22. – Art. 4504. https://doi.org/10.3390/electronics14224504.
6. Focardi R. A formally verified configuration for hardware security modules in the cloud / R. Focardi, F.L. Luccio // Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '21). – 2021. – P. 412-428. https://doi.org/10.1145/3460120.3484750.
7. A trusted execution environment RISC-V system-on-chip compatible with transport layer security 1.3 / B. Kieu-Do-Nguyen et al // Electronics. – 2024. – Vol. 13, № 13. – Art. 2508. https://doi.org/10.3390/electronics13132508.
8. Profiled side channel attacks against the RSA cryptosystem using neural networks / A. Barenghi et al // Journal of Information Security and Applications. – 2022. – Vol. 66. – Art. 103122. https://doi.org/10.1016/j.jisa.2022.103122.
9. Enhanced side-channel analysis on ECDSA employing fixed-base comb method / S. Jin et al // IEEE Transactions on Computers. – 2022. – Vol. 71, № 9. – P. 2341-2350. https://doi.org/10.1109/TC.2021.3126387.
10. A novel and efficient SPI enabled RSA crypto accelerator for real-time applications / V.R. Kolagatla et al // Proceedings of the 28th International Symposium on VLSI Design and Test (VDAT). – 2024. – P. 1-6.
11. Hardware performance analysis of RSA cryptosystems on FPGA for wireless sensor nodes / G. Leelavathi et al // International Journal of Intelligent Networks. – 2021. – Vol. 2. – P. 184-194. https://doi.org/10.1016/j.ijin.2021.09.002.
12. Optimized RSA-1024 FPGA implementation on Artix-7 / R. Ghayoula et al // Coding Theory – Advances and Applications in Informatics, Data Analysis, and Cryptography. – 2025. – Vol. 6. – P. 244.
13. Efficient FPGA-based ECDSA verification engine for permissioned blockchains / R. Agrawal et al // IEEE ASAP. – 2022. – P. 148-155. https://doi.org/10.1109/ASAP54618.2022.00028.
14. Cryptographic accelerators for digital signature based on Ed25519 / M. Bisheh-Niasar et al // IEEE Transactions on VLSI Systems. – 2021. – Vol. 29, № 7. – P. 1297-1305. https://doi.org/10.1109/TVLSI.2021.3071086.
15. A hardware efficient elliptic curve accelerator for FPGA based cryptographic applications / M. Kashif et al // ELECO. – 2019. – P. 362-366.
16. Rodionov A.Yu. Arxitektura kriptograficheskogo soprocessora na PLIS / A.Yu. Rodionov // Voprosy` zashhity` informacii. – 2016. – № 3(114). – S. 16-19. Development of optical transceivers SFF standard with support for cryptographic kernel / I.A. Kashirin et al // APEIE. – 2016. – P. 159-162. (In Russian).
17. Debugging and verifying SoC designs through effective cross-layer hardware-software co-simulation / K. Campbell et al // DAC. – 2016. – P. 1-6. https://doi.org/10.1145/2897937.2898068.
18. Hardware and software co-verification from security perspective in SoC platforms / K. Chen et al // Journal of Systems Architecture. – 2022. – Vol. 122. – Art. 102355. https://doi.org/10.1016/j.sysarc.2021.102355.
19. Verification of SoC using advanced verification methodology / P. Pamula et al // Engineering Proceedings. – 2023. – Vol. 34, № 1. – Art. 12. https://doi.org/10.3390/engproc2023034012.
20. Verification of an ARM Cortex-M3 based SoC using UVM / A. Hegazy et al // SPIN. – 2023. – P. 778-783. https://doi.org/10.1109/SPIN57001.2023.10116603.

21. Farooq U., Mehrez H. Pre-silicon verification using multi-FPGA platforms: a review // Journal of Electronic Testing. – 2021. – Vol. 37. – P. 7–24. https://doi.org/10.1007/s10836-020-05904-8.
22. Makinote: an FPGA-based HW/SW platform for pre-silicon emulation of RISC-V designs / E. Perdomo et al // RAPIDO. – 2024. – P. 29-34.
23. FPGA prototyping of heterogeneous security architecture for educational purposes / S. Stoyanov et al // Engineering Proceedings. – 2025. – Vol. 100, № 1. – Art. 18. https://doi.org/10.3390/engproc2025100018.
24. Open-source design of integrated circuits / P. Fath et al // e+i Elektrotechnik und Informationstechnik. – 2024. – Vol. 141. – P. 76-87. https://doi.org/10.1007/s00502-023-01185-7.
25. Integrating design for testability technique into OpenLane with Skywater 130-nm process design kit / K. Chew et al // Semarak Engineering Journal. – 2023. – Vol. 3, № 1. – P. 14-21.
26. Custom ASIC design for SHA-256 using open-source tools / L.D. Franck et al // Computers. – 2024. – Vol. 13, № 1. – Art. 9. https://doi.org/10.3390/computers13010009.
27. A survey on assertion-based hardware verification / W. Hasini et al // ACM Computing Surveys. – 2022. – Vol. 54, № 11. – P. 1-33. https://doi.org/10.1145/3484517.
28. DirectFuzz: automated test generation for RTL designs using directed graybox fuzzing / S. Canakci et al. // DAC. – 2021. – P. 529-534. https://doi.org/10.1109/DAC18074.2021.9586230.
29. SoCFuzzer: SoC vulnerability detection using cost function enabled fuzz testing / M.M. Hossain et al. // DATE. – 2023. – P. 1-6. https://doi.org/10.23919/DATE56975.2023.10137021.
30. DifuzzRTL: differential fuzz testing to find CPU bugs / J. Hur et al // IEEE Symposium on Security and Privacy. – 2021. – P. 1286-1303. https://doi.org/10.1109/SP40001.2021.00063.
31. SHarPen: SoC security verification by hardware penetration test / H. Al-Shaikh et al // ASPDAC. – 2023. – P. 579-584. https://doi.org/10.1109/ASPDAC56680.2023.10044776.
32. Remote WebAuthn: FIDO2 authentication for less accessible devices / P. Wagner et al // ICISSP. – 2023. – P. 368-375. https://doi.org/10.5220/0011624500003405.
33. A novel protocol using captive portals for FIDO2 network authentication / M. Rivera-Dourado et al // Applied Sciences. – 2024. – Vol. 14, № 9. – Art. 3610. https://doi.org/10.3390/app14093610.
34. GlobalShuttle™: Multi Project Wafer Program. https://gf.com/manufacturing-services/multi-project-wafer-program/ (дата обращения: 08.02.2026).
35. Offered MPW services – Si CMOS, compound semiconductor. https://www.mosis2.com/mpw-services (дата обращения: 08.02.2026).
36. TSMC MPW shared tapeouts. https://www.musesemi.com/shared-block-tapeout-pricing (дата обращения: 08.02.2026).
37. Cadence and SkyWater: fostering the next generation of innovators. https://community.cadence.com/... (дата обращения: 08.02.2026).
38. Tiny Tapeout. https://tinytapeout.com/chips/ (дата обращения: 08.02.2026).
39. Venn M. Tiny Tapeout: a shared silicon tape-out platform accessible to everyone / M. Venn // IEEE Solid-State Circuits Magazine. – 2024. – Vol. 16, № 2. – P. 20-29. https://doi.org/10.1109/MSSC.2024.3371234.
40. Cocotb. https://www.cocotb.org/ (дата обращения: 08.02.2026).

Информация о финансировании

Данное исследование финансируется Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP26103891).

И.А. Сенюшин[1], Н.С. Глазырина[1]*, Р.Б. Ибраев[1], Е.К. Джилкибаев[1], А. Әділғазыұлы[2]
[1]«TSARKA R&D» ЖШС
010000, Қазақстан Республикасы, Астана қ., Қабанбай батыр даңғылы, 51/1
[2]Назарбаев университеті,
010000, Қазақстан Республикасы, Астана қ., Қабанбай батыр даңғылы, 53
*e-mail: glazirinan@yandex.ru

ЭЛЕКТРОНДЫҚ ЦИФРЛЫҚ ҚОЛТАҢБАҒА АРНАЛҒАН КРИПТОГРАФИЯЛЫҚ КОНТРОЛЛЕРДІ ӘЗІРЛЕУДІҢ ФОРМАЛДАНДЫРЫЛҒАН БАҒДАРЫ АППАРАТТЫҚ ППВМ ВЕРИФИКАЦИЯСЫМЕН

Бұл мақалада электрондық цифрлық қолтаңбаларды аппараттық іске асыруға арналған мамандандырылған криптографиялық контроллер үшін формалдандырылған әзірлеу ағыны

ұсынылады және эксперименттік түрде тексеріледі. Ұсынылған бағдар криптографиялық контроллерді әзірлеудің толық циклін қамтиды және архитектуралық синтезді, RTL іске асыруды, ППВМ (Пайдаланушы Программалайтын Вентильді Матрица) верификацияны және MPW ағынында физикалық іске асыруды біріктіреді. Контроллер архитектурасы модульдік принципті қолдану арқылы әзірленген, мұнда жүйе жеке модульдер ретінде әзірленген және верификацияланған функционалдық тәуелсіз аппараттық блоктар жиынтығымен ұсынылған. Әрбір модуль ППВМ түптүрлілеу кезінде RTL іске асырудан, бағдарламалық интерфейсті қалыптастырудан және аппараттық верификациядан өтеді. Бұл әзірлеудің басында функционалдық және интерфейс қателерін анықтауға мүмкіндік береді. Маңызды модульдер RTL-GDS ағынында қосымша DRC және LVS физикалық жобалау верификацияларынан өтеді. Модульдік верификациядан кейін блоктар біріктіріледі, жад картасы жасалады және жүйенің аппараттық верификациясы орындалады. Ұсынылған тәсілдің эксперименттік тексеруі GOWIN Tang Primer 20K және TinyTapeout (PDK SkyWater SKY130) платформаларын пайдаланып TinyQV (RISC-V) ядросына негізделген демонстрациялық есептеу модулінде жүргізілді. Нәтижелер ұсынылған тәсілдің қайталану мүмкіндігін және оның мамандандырылған криптографиялық контроллерлер мен қауіпсіз кірістірілген жүйелерді әзірлеу үшін қолданылуын растайды.

Түйін сөздер: *криптографиялық контроллер, электрондық цифрлық қолтаңба, ППВМ түптүрлілеу, аппараттық верификация, MPW-түптүрлілеу, ақпараттық қауіпсіздік.*

I. Seniushin[1], N. Glazyrina[1]*, R. Ibrayev[1], Jilkibayev[1], A. Adilgazyuly[2]
[1]TSARKA R&D LLP,
Republic of Kazakhstan, Astana, 51/1 Kabanbai Batyr Avenue
[2]Nazarbayev University,
Republic of Kazakhstan, Astana, 53 Kabanbai Batyr Avenue
*e-mail: glazirinan@yandex.ru

FORMALIZED DEVELOPMENT FLOW FOR A CRYPTOGRAPHIC CONTROLLER WITH DIGITAL SIGNATURE AND FPGA-BASED VERIFICATION

This article presents and experimentally validates a formalized development flow for a specialized cryptographic controller designed for hardware implementation of digital signature algorithms. The flow covers the complete design cycle, encompassing architectural synthesis, RTL implementation, FPGA-based hardware verification, and physical implementation within an MPW flow. The controller architecture follows a modular design principle, in which the system is decomposed into functionally independent hardware blocks that are developed and verified individually. For each block, RTL implementation, software interface generation, and hardware verification are carried out during FPGA prototyping, enabling early detection of functional and interface errors. Critical components undergo additional physical verification through an RTL-to-GDS flow, including DRC and LVS checks. Upon completion of modular verification, the blocks are integrated, a memory map is generated, and system-level hardware verification is performed. The approach was experimentally validated on a demonstration computing module based on the TinyQV (RISC-V) core, using the GOWIN Tang Primer 20K and TinyTapeout (PDK SkyWater SKY130) platforms. The results confirm the reproducibility of the proposed flow and its practical applicability for developing specialized cryptographic controllers and secure embedded systems.

Key words: *cryptographic controller, electronic digital signature, FPGA prototyping, hardware verification, MPW prototyping, information security.*

Сведения об авторах

Игорь Анатольевич Сенюшин – проектный менеджер, ТОО «TSARKA R&D», г. Астана, Республика Казахстан; e-mail: sigor@cybersec.kz. ORCID: https://orcid.org/0009-0008-4479-4478.

Наталья Сергеевна Глазырина* – PhD, ассоциированный профессор, координатор научный проектов, ТОО «TSARKA R&D», г. Астана, Республика Казахстан; e-mail: glazirinan@yandex.ru. ORCID: https://orcid.org/0000-0002-0259-774X.

Ренат Булатович Ибраев – специалист по криптографической безопасности, ТОО «TSARKA R&D», г. Астана, Республика Казахстан; e-mail: crypto.teacher2020@gmail.com. ORCID: https://orcid.org/0000-0002-7800-9035.

Ерболсын Кайратович Джилкибаев – руководитель отдела разработки, ТОО «TSARKA R&D», г. Астана, Республика Казахстан; e-mail: yerbolsyn@proton.me. ORCID: https://orcid.org/0009-0003-2797-1421.

Алмас Әділғазыұлы – студент школы инженерии и цифровых наук, Назарбаев университет; e-mail: almas.adilgazyuly@nu.edu.kz. ORCID: https://orcid.org/0009-0000-1196-7952.

Авторлар туралы мәліметтер

Игорь Анатольевич Сенюшин – «TSARKA R&D» ЖШС жоба жетекшісі, Астана, Қазақстан Республикасы; e-mail: sigor@cybersec.kz. ORCID: https://orcid.org/0009-0008-4479-4478.

Наталья Сергеевна Глазырина* – PhD докторы, доцент, «TSARKA R&D» ЖШС ғылыми жоба үйлестірушісі, Астана қ., Қазақстан Республикасы; e-mail: glazirinan@yandex.ru. ORCID: https://orcid.org/0000-0002-0259-774X.

Ренат Булатович Ибраев – криптографиялық қауіпсіздік маманы, «TSARKA R&D» ЖШС, Астана қ., Қазақстан Республикасы; e-mail: crypto.teacher2020@gmail.com. ORCID: https://orcid.org/0000-0002-7800-9035.

Ерболсын Кайратович Джилкибаев – әзірлеу бөлімінің басшысы, «TSARKA R&D» ЖШС, Астана қ., Қазақстан Республикасы; e-mail: yerbolsyn@proton.me. ORCID: https://orcid.org/0009-0003-2797-1421.

Алмас Әділғазыұлы – Инженерия және цифрлық ғылымдар мектебінің студенті, Назарбаев Университеті, Астана қ., Қазақстан Республикасы; e-mail: almas.adilgazyuly@nu.edu.kz. ORCID: https://orcid.org/0009-0000-1196-7952.

Information about the authors

Igor Seniushin – Project Manager, TSARKA R&D LLP, Astana, Republic of Kazakhstan; e-mail: sigor@cybersec.kz. ORCID: https://orcid.org/0009-0008-4479-4478.

Natalya Glazyrina* – PhD, associate professor, scientific project coordinator, TSARKA R&D LLP, Astana, Republic of Kazakhstan; e-mail: glazirinan@yandex.ru. ORCID: https://orcid.org/0000-0002-0259-774X.

Renat Ibrayev – Cryptographic Security Specialist, TSARKA R&D LLP, Astana, Republic of Kazakhstan; e-mail: crypto.teacher2020@gmail.com. ORCID: https://orcid.org/0000-0002-7800-9035.

Yerbolsyn Jilkibayev – Head of Development Department, TSARKA R&D LLP, Astana, Republic of Kazakhstan; e-mail: yerbolsyn@proton.me. ORCID: https://orcid.org/0009-0003-2797-1421.

Almas Adilgazyuly – Student, School of Engineering and Digital Sciences, Nazarbayev University, Astana, Republic of Kazakhstan; e-mail: almas.adilgazyuly@nu.edu.kz. ORCID: https://orcid.org/0009-0000-1196-7952.

Поступила в редакцию 30.03.2026
Поступила после доработки 23.04.2026
Принята к публикации 24.04.2026

https://doi.org/10.53360/2788-7995-2026-2(22)-3

ҒТАХР: 28.23.37

А. Хабай[1], Е.А. Тулешов[1], А.Е. Назырова[2], Ж.Н. Исабеков*[1], С.Е. Ибекеев[1,3]
[1]Satbayev University,
050013, Қазақстан Республикасы, Алматы қаласы, Сәтбаев көшесі, 22а
[2]Л.Н. Гумилёв атындағы Еуразия ұлттық университеті,
10000 Қазақстан Республикасы, Астана қ., Сәтбаев к-сі, 2
[3]Алматы Технологиялық Университеті,
Қазақстан Республикасы, Алматы, Төле би көшесі, 100
*e-mail: z.issabekov@satbayev.university

ҰШҚЫШСЫЗ ҰШУ АППАРАТТАРЫНА АҒЫНДЫҚ ДЕРЕКТЕРДІ БЕРУ ҮШІН MIMO ӘДІСІН ҚОЛДАНУДЫ ТАЛДАУ

Аңдатпа: *Мақалада ұшқышсыз ұшу аппараттары (ҰҰА) үшін екі жолақты көп кірісті және көп шығысты антенна жүйесінің өнімділігі жан-жақты талданды. ҰҰА мен жердегі басқару орталықтары арасындағы жоғары жылдамдықты және сенімді деректер тасымалын қамтамасыз ету қазіргі заманғы байланыс технологияларының басты міндеттерінің бірі болып табылады.*