Московский физико-технический институт
(государственный университет)

Аппаратные решения для задач защиты информации

Автор: Дедков Денис Андреевич
студент Б01-108

Долгопрудный, 2024

Содержание

1 Введение

Разработка и использование специализированных аппаратных решений для своих нужд в последнее время набирает популярность. Такие чипы быстро проникают во все сферы нашей жизни, вытесняя решения общего назначения. Игнорирование этого факта в скором времени сделает существующие решения неконкурентоспособными.

Основные задачи данной работы - показать преимущества такой специализированной аппаратуры в сфере защиты информации и отобразить проблематику использования решений общего назначения. С этой целью проводится обзор существующих передовых продуктов с количественными характеристиками и ссылками на научные работы, показывающие эффективность конкретных реализаций. Акцент поставлен на применение чипов в развивающихся областях, по возможности описываются актуальные проблемы в этих сферах.

Для систематизации знаний также предлагается провести классификацию таких аппаратных решений.

2 Причины использования аппаратных решений

Когда речь идет об аппаратных решениях, чаще всего имеют в виду ASIC (Application-Specific Integrated Circuit, интегральная схема специального назначения). Такие микросхемы выполняют строго ограниченные функции. Вследствие этого выполнение функций происходит более эффективно. Следствием специализации также является конечная стоимость производства таких чипов: она может быть на порядки меньше стоимости чипа общего назначения.

Любому, будь то SoC (System on Chip, Система на Кристалле) или ASIC, решению соответствует точка в пространстве PPA (Power, Performamce, Area). [1] По расположению чипа в этом пространстве, можно определить его специализацию, или мощность множества задач, который данный чип эффективно может решать при реалистичной стоимости производства (см. рис. 1). Именно с этой точки зрения ASIC решения являются наиболее выгодными.

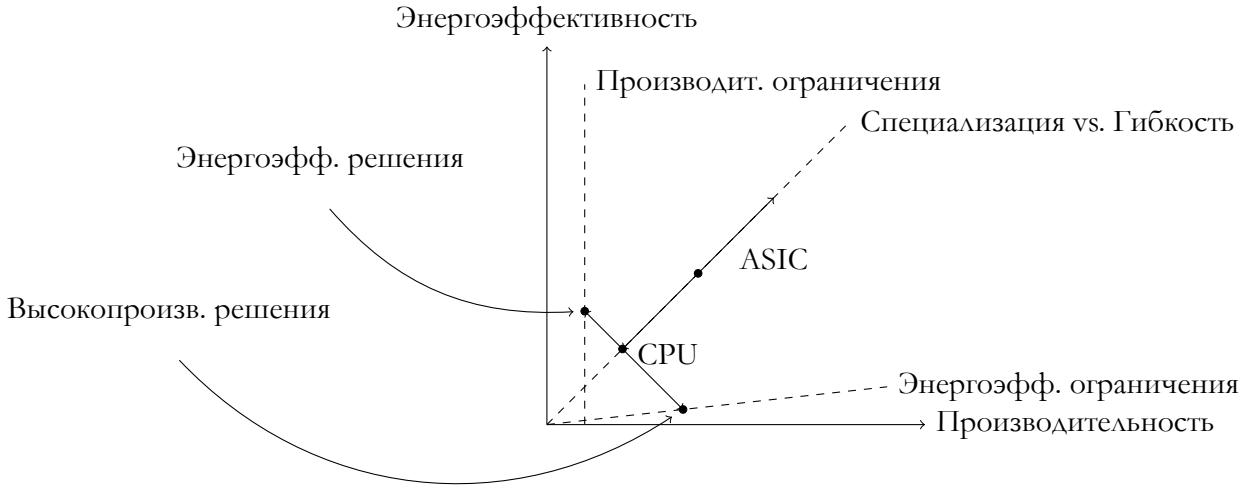

Рис. 1: Пространство вычислителей. Рисунок на основе курса [1].

[1] Энергопотребление, производительность и площадь чипа.

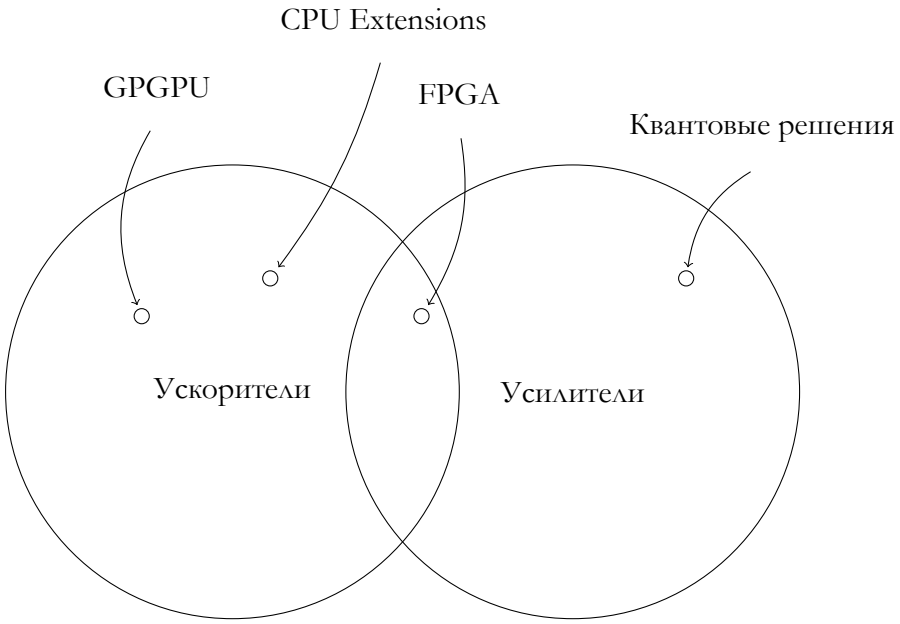

Рис. 2: Классы аппаратных решений.

Не удивителен тот факт, что специализированные аппаратные решения востребованы и в сфере защиты информации, включающей в себя огромные массивы вычислительных задач. А применение таких чипов продолжает набирать популярность.

Предлагается разделить существующие аппаратные решения на два пересекающихся класса: **ускорители** и **усилители**.

Основное применение ускорителей - улучшение производительности систем защиты информации. Чаще всего под этим подразумевается ускорение работы существующих криптографических алгоритмов. Чистые ускорители не привносят новые механизмы защиты и, с точки зрения функциональности, могут быть заменены решениями общего назначения.

Основное применение усилителей - улучшение безопасности систем защиты информации. Такое усиление может достигаться как путем изоляции криптографических вычислений, так и исключительно новыми подходами в обеспечении защиты, вроде применения физических принципов. Такие решения могут работать существенно медленней систем на основе чипов общего назначения, однако их использование приводит к колоссальному росту защищенности, что и является основной причиной их использования.

На рисунке 2 отображены классы решений и некоторые их реализации, обзор которых и является одной из основных целей данной работы.

3 Обзор существующих аппаратных решений

3.1 Расширения CPU

Производители центральных процессоров общего назначения (General-purpose CPU) интегрируют в чип специализированные блоки, позволяющие ускорять вычисления. Такие микроархитектурные изменения отображаются в архитектуре расширением системы команд.

Есть две основных причины успеха такого рода расширений: использование широких регистров (длиной 128 бит и более) и внедрение специальных вычислительных блоков.

Векторные регистры позволяют производить вычисления над пачкой из нескольких 8, 16, 32 или 64-битных чисел одновременно, улучшая тем самым пропускную способность (bandwidth) чипа.

Специализация позволяет заменить последовательность из десятка операций центрального процессора общего назначения на одну-две инструкции, исполняемые на отдельном вычислительном блоке, чем уменьшает общее время, требуемое на совершение операции (latency).

Два десятилетия назад началось внедрение расширений CPU [2], что привело к удачной коллекции векторных расширений: MMX, SSE, AVX архитектур Intel 64 и AMD64, Neon расширение архитектуры Arm, расширение V системы команд RISC-V. Векторные расширения, позволяя ускорять вычисления в десятки раз, завоевали большую популярность, чем положили начало массовому росту количества и разнообразия таких расширений.

Как следствие был создан целый набор расширений для задач защиты информации: Intel SHA (SHA-1, SHA-256, SHA-512), AES. К примеру, Arm v8 Crypto Extensions показывают ускорение SHA2-256 до $6x$ относительно оригинального алгоритма на процессоре общего назначения, в зависимости от размера блока [2].

Недавно актуальная задача создания расширений для криптографии стояла и перед дизайнерами архитектуры RISC-V [3], что привело к созданию документа RISC-V Cryptography Extensions в 2021. Расширение включает в себя набор инструкций для ускорения алгоритмов AES, SM4 Block Cipher. Вычислений в полях: Carry-less multiply, Bitmanip instructions for Cryptography и пр [4].

Расширяемая природа архитектуры RISC-V позволяет создавать и реализовывать собственные расширения системы команд. И такие расширения активно создаются. Примером может служить криптографическое расширение LightWeight Cryptography (LWC) от Национального института стандартов и технологий США (The National Institute of Standards and Technology, NIST) для использования в IoT (интернет вещей, internet of things) [5].

Не смотря на существенное ускорение, вычисление на CPU векторов более 512 бит приводит к экспоненциальному росту сложности проектирования чипа. Этот факт является принципиальным ограничением криптографических систем на основе процессоров общего назначения. В этом смысле инициатива перешла к более узкоспециализированным вычислителям, вроде GPGPU.

3.2 GPGPU

GPGPU (General-purpose computing on graphics processing units) — использование графического процессора видеокарты, предназначенного для компьютерной графики, в целях производства математических вычислений, которые обычно проводит центральный процессор (CPU). Аппаратные решения, реализующие данную технологию, позволяют эффективно использовать параллелизм решаемых задач. Наиболее широко такие чипы используются в сфере машинного обучения.

Список производителей данных вычислителей: NVIDIA, AMD, Cerebras, Google, Intel, Biren. Однако на текущий момент более 80% мирового рынка производителей GPGPU вычислителей занято компанией NVIDIA. А ключевую роль в этом играет CUDA (Compute Unified Device Architecture) – программная модель NVIDIA. И на сегодняшний день альтернатив

Классические криптографические алгоритмы, вроде RSA и AES, успешно оптимизируются под вычисления на существующих GPGPU решениях. CUDA реализации данных

[2] Речь идет о MMX расширении процессоров компании Intel.

алгоритмов осуществляют на порядки превосходят передовые CPU решения.

Параллельная RSA-расшифровка данных с применением видеокарт NVIDIA показывает 1197.5x ускорение относительно CPU [6]. Скорость шифрования в AES достигает значений в 200Gbps [7] [8], что в десятки раз превосходит оптимизированные CPU реализации с использованием Intel AES Extension.

Гетерогенные вычисления AES с применением связки CPU-GPU показывают снижение энергопотребления на 74% в сравнении с CPU-only решением и на 21% в сравнении с GPU-only системами [9].

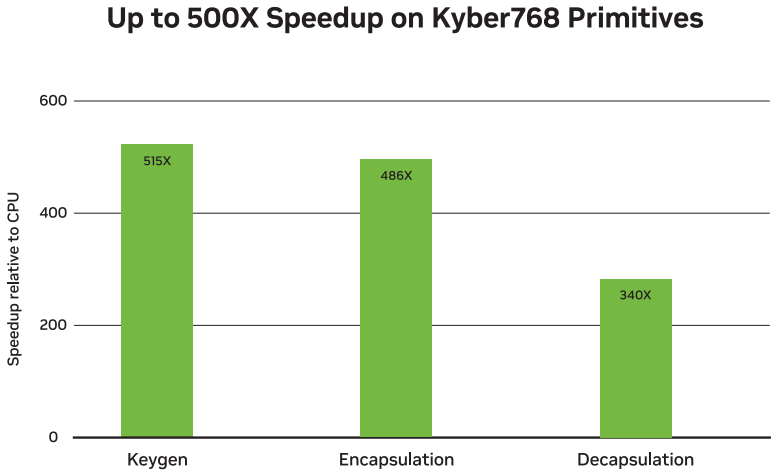

Рис. 3: Измерения на чипе NVIDIA H100. Сравнение с современными однопоточными процессорами, используемыми в тестовом пакете liboqs [10].

Недавнее сотрудничество компании QuSecure, лидера в сфере постквантовой криптографии, с компанией NVIDIA, привело к серьезным шагам в сторону адаптации GPGPU вычислителей для задач «Постквантовой Эры» [11]. Одно из основных достижений в рамках сотрудничества – создание CUDA cuPQC – SDK (Software Development Kit) оптимизированных библиотек для ускорения передовых постквантовых алгоритмов. Заявляется $300 - 500x$ ускорение алгоритма Kyber 768 относительно оптимизированных с помощью Intel AVX реализаций (см. рис. 3).

3.3 Квантовые решения

На текущий момент существует два класса задач, которые успешно решаются существующими квантовыми решениями: генерация случайных чисел (ГСЧ) и квантовое распределение ключей.

Генерация случайных чисел

Важность генерации случайных чисел сложно переоценить. Случайные числа являются важнейшим ресурсом в огромном числе практических приложений. Последовательности случайных чисел применяются в системах безопасности, криптографии, в научных исследованиях (статистике, моделировании различных систем и процессов).

Генераторы случайных чисел традиционно делят на две категории: аппаратные (АГСЧ, англ. hardware random number generator, HRNG) и псевдослучайные (ПГСЧ, англ. pseudorandom number generator, PRNG).

Устройства, основанные на макроскопических случайных процессах, не могут обеспечить скорости получения случайных чисел, достаточной для прикладных задач. Поэтому в основе современных АГСЧ лежат источники шума, из которых извлекаются случайные биты: дробовой шум, радиоактивный распад, спонтанное параметрическое рассеяние [12].

Основная проблема аппаратных генераторов случайных чисел — это их относительно медленная по сравнению с генераторами псевдослучайных последовательностей работа. Также многие из них постепенно деградируют со временем, а анализ и верификация таких генераторов задача весьма затруднительная.

Квантовые генераторы случайных чисел (КГСЧ) в качестве физического источника энтропии используют квантовые процессы, которые сами по себе имеют вероятностную природу, что делает их идеально подходящими для криптографических приложений.

Решения Quantis QRNG Chip ветерана отрасли – компании ID Quantique (IDQ), достигают скорости генерации $20Mb/s$ [13]. Не уступает им и ближайший конкурент Crypta Labs, предоставляя генераторы Firefly PCIe QRNG со скоростью генерации до $20Mb/s$ [14].

Если требуется высокая скорости генерации, то по этому критерию на порядок обходит конкурентов компания Quantum Dice со своими генераторами VERTEX 1100 [15] и APEX 2100 [16], достигающими скорости генерации случайной последовательности бит $2.66Gb/s$ и $7.5Gb/s$ соответственно.

Активная работа по созданию передового КГСЧ сегодня ведется отечественной компанией QRate. Скорость их решения QRate Chaos будет превышать $1Gb/s$ [17].

Квантовое распределение ключей

Генерация общего ключа является краеугольным камнем любой симметричной криптосистемы. Задача безопасной передачи с последующим хранением ключа обладает высочайшей сложностью. Всегда существует риск утраты конфиденциальности, связанный с компрометацией ключа, в том числе и неявной: увольнение сотрудника, который имел допуск к ключевой информации, необходимость допуска сотрудников других организаций и так далее. Чем дольше используется один и тот же ключ, тем выше вероятность того, что он уже явно или неявно скомпрометирован. Но помимо риска компрометации при длительном использовании одного и того же ключа существует ограничение на объем шифруемой информации. После исчерпания ключа, взлом можно попытаться осуществить статистическими методами.

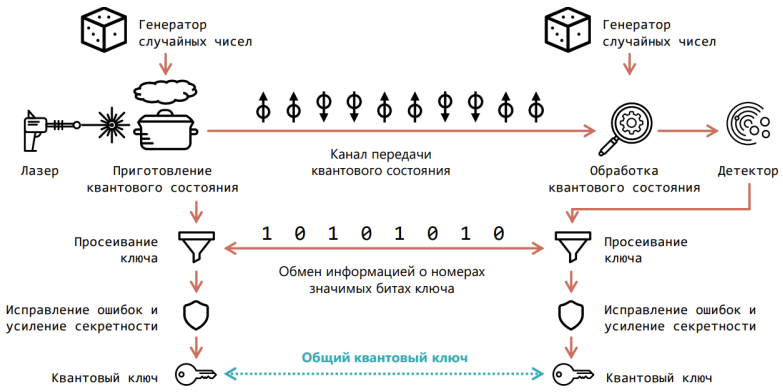

Рис. 4: Квантовое распределение ключей. Принцип действия [18].

Предложенное Стивеном Визнером (англ. Stephen Wiesner) в 1983 г. решение проблемы

генерации общего секрета, используя квантовые принципы, оказалось весьма удачным [19]. Последующая разработка привела к созданию алгоритмов квантового распределения ключей (КРК) — семейства криптографических протоколов, позволяющих двум удаленным абонентам выработать общий случайный секрет (ключ).

Гарантия безопасности квантового распределения ключей заложена в протоколе фундаментально. Считается, что секретность выработки квантовых ключей основана на следующих принципах:

1. Невозможно клонировать неизвестное квантовое состояние.
2. Невозможно различить два неортогональных квантовых состояния.
3. Невозможно измерить квантовое состояние без его изменения (редукция волновой функции).

Эти принципы позволяют гарантированно детектировать пассивного/активного злоумышленника, что делает невозможным атаку «человек по середине», другими словами незаметную компрометацию ключа шифрования.

Протокол КРК имеет ряд существенных преимуществ перед классическими протоколами передачи секрета: доказанная секретность квантовых ключей, отсутствие необходимости в постоянном администрировании, стойкость к криптографическим атакам с применением квантового компьютера, высокая скорость смены ключей.

Аппаратные решения, реализующие протокол квантового распределения ключей, являются типичными представителями класса усилителей, обеспечивая надежное создание криптографического ключа на узлах. Схема общепринятой организации протокола приведена на рисунке 4.

В конце 2020 года компания «ИнфоТеКС» совместно с физическим факультетом МГУ имени М.В. Ломоносова представили лабораторные образцы ViPNet Quandor - коммерческого отечественного комплекса, работающего в топологии «точка-точка», включающего аппаратуру для КРК [20]. Современный приемник ViPNet Quandor 2, обладает скоростью выработки квантовых ключей 256 бит/мин с максимальной длиной квантового канала 100 км [21]. Наращивание компетенций компании привело к созданию ViPNet Quantum Trusted System (ViPNet QTS) - решению для создания квантовой криптографической сети произвольной топологии [22].

Компания ID Quantique (IDQ), лидер в области квантовой коммуникации, продает свои реализации протокола квантового распределения ключей. Передовое решение Clavis XG QKD System предлагает длину канала до 150 км с поддержкой произвольных топологий. Более приземленная аппаратура Cerberis XG QKD System обладает каналом до 90 км [23].

4 Заключение

В работе были определены основные причины использования аппаратных решений, акцент поставлен на применение в области защиты информации. Описана идея баланса процесса разработки аппаратуры в терминах PPA (Power, Performamce, Area).

Проведена классификация аппаратных решений для задач защиты информации - разбиение на два пересекающихся класса: усилители и ускорители.

Был проведен обзор существующих передовых решений в классе ускорителей: расширения центрального процессора (CPU) и графические процессоры общего назначения (GPGPU).

Дано описание задач, эффективно решаемых квантовыми системами: квантовые генераторы случайных чисел и квантовое распределение ключей. Приведены актуальные аппаратные реализации квантовых протоколов.

За рамками данной работы осталась интересная область аппаратуры для защиты информации на основе программируемых логических интегральных схем (ПЛИС, англ. FPGA), которые обладают существенно укороченным циклом разработки, что приводит к разнообразию таких чипов.

Список литературы

[1] S. o. E. Cornell University and C. Engineering, "Ece 5745 complex digital asic design spring 2023." [Online]. Available: https://www.csl.cornell.edu/courses/ece5745/handouts.html

[2] AMD, "Accelerating cryptographic performance on versal adaptive socs," November 2023.

[3] B. Marshall, G. R. Newell, D. Page, M.-J. O. Saarinen, and C. Wolf, "The design of scalar AES instruction set extensions for RISC-V," vol. 2021, no. 1, Dec. 2020, pp. 109–136, artifact available at https://artifacts.iacr.org/tches/2021/a3.

[4] R.-V. International, "Risc-v cryptography extensions volume i: Scalar entropy source instructions," 2021.

[5] E. Tehrani, T. Graba, A. S. Merabet, and J.-L. Danger, "Risc-v extension for lightweight cryptography," in *2020 23rd Euromicro Conference on Digital System Design (DSD)*, 2020, pp. 222–228.

[6] Y.-S. Lin, C.-Y. Lin, and D.-C. Lou, "Efficient parallel rsa decryption algorithm for many-core gpus with cuda," 01 2012.

[7] A. Abdelrahman, M. Fouad, H. Dahshan, and A. Mousa, "High performance cuda aes implementation: A quantitative performance analysis approach," 07 2017.

[8] A. Abdelrahman, M. Fouad, G. Salama, and H. Dahshan, "Enhancing the actual throughput of the aes algorithm on the pascal gpu architecture," 10 2018.

[9] X. Fei, K. Li, W. Yang, and K. Li, "Analysis of energy efficiency of a parallel aes algorithm for cpu-gpu heterogeneous platforms," vol. 94-95, 2020, p. 102621. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167819120300144

[10] "Nvidia cupqc." [Online]. Available: https://developer.nvidia.com/cupqc

[11] "Make it so: Software speeds journey to post-quantum cryptography." [Online]. Available: https://blogs.nvidia.com/blog/cupqc-quantum-cryptography/

[12] H. Tilborg and S. Jajodia, *Encyclopedia of Cryptography and Security, 2nd Ed*, 01 2011.

[13] I. Quantique, "Quantis qrng chips." [Online]. Available: https://marketing.idquantique.com/acton/attachment/11868/f-025e/1/-/-/-/-/Quantis%20QRNG%20Chip_Brochure.pdf

[14] C. Labs, "Firefly pcie quantum random number generator." [Online]. Available: https://cryptalabs.com/support/docs/brochures/CryptaLabs_Pcie_QRNG_SpecSheet.pdf

[15] "Quantum dice. vertex 1100." [Online]. Available: https://www.quantum-dice.com/vertex/

[16] "Quantum dice. apex 2100." [Online]. Available: https://www.quantum-dice.com/apex-1/

[17] "Qrate chaos - квантовый генератор случайных чисел (pat. №2721585)." [Online]. Available: https://goqrate.com/projects/qrate-chaos-kvantovyy-generator-sluchaynykh-chisel-pat-2721585/

[18] "Квантовые продукты ИнфоТеКС." [Online]. Available: https://infotecstechfest.ru/upload/iblock/20f/tvtc2bzrgt8sr9fk27myjwo1o4yudjww.pdf

[19] W. S., "Conjugate coding," 1983, pp. 78 – 88.

[20] "Vipnet quandor прошел испытания на соответствие требованиям технического регламента ЕАЭС." [Online]. Available: https://quantum.msu.ru/ru/press/news/2021-10/quandor-eaes

[21] "Vipnet quandor 2 - квантовая криптографическая система выработки и распределения ключей с топологией «точка-точка»." [Online]. Available: https://infotecs.ru/products/vipnet-quandor-2/

[22] "Vipnet qts - решение для создания квантовой криптографической сети произвольной топологии." [Online]. Available: https://infotecs.ru/products/vipnet-qts/

[23] "Id quantique (idq) - quantum key distribution." [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/#key_exchange_service