О ПРИМЕНИМОСТИ ПОСТКВАНТОВОГО СТАНДАРТА ЭЛЕКТРОННОЙ ПОДПИСИ SLH-DSA В СМАРТ-КАРТАХ

Панасенко С. П.[1]

DOI: 10.21681/2311-3456-2025-3-29-37

Цель работы: *проанализировать влияние стандартного протокола обмена со смарт-картами на применимость ресурсоемких постквантовых алгоритмов электронной подписи в устройствах с ограниченными ресурсами на примере смарт-карт и дать рекомендации по модернизации стандартного протокола по результатам анализа.*

Методы исследования: *теория информации, системный анализ, объектно-ориентированный анализ.*

Результаты исследования: *проанализированы различные сценарии взаимодействия со смарт-картой при использовании стандартного протокола обмена на примере выполнения смарт-картой функции вычисления электронной подписи стандартизованным в США постквантовым алгоритмом SLH-DSA; в результате анализа показаны ограничения стандартного протокола обмена, напрямую препятствующие применимости алгоритма SLH-DSA (и схожих с ним по характеристикам алгоритмов) в смарт-картах.*

Научная новизна: *по результатам проведенного анализа предложено направление модернизации стандартного протокола обмена со смарт-картами для его адаптации к характеристикам ресурсоемких постквантовых алгоритмов электронной подписи; предложенная модернизация протокола позволит использовать ряд постквантовых криптоалгоритмов в смарт-картах.*

Ключевые слова: *электронная подпись, постквантовая криптография, смарт-карта, протокол APDU, алгоритм SLH-DSA.*

Введение

Значительная часть традиционных асимметричных криптоалгоритмов базируется на сложности факторизации целых чисел или дискретного логарифмирования, в т. ч. в группе точек эллиптической кривой. Данные проблемы могут быть легко разрешимы с помощью алгоритмов для квантовых или гибридных вычислений, основанных на алгоритме Шора [1], при условии появления квантового компьютера, обладающего достаточными ресурсами. На текущий момент такие компьютеры по-прежнему являются гипотетическими, но технический прогресс в области их создания выглядит очевидным – уже сейчас с помощью существующих квантовых компьютеров (ресурсов которых пока, в общем случае, недостаточно для успешного криптоанализа реально используемых систем) решаются различные задачи с использованием эффекта квантового превосходства – см., например, [2].

В отчете [3] эксперты международной консалтинговой компании McKinsey предполагают, что к 2030 г. появятся квантовые компьютеры достаточной мощности для успешного криптоанализа реально применяемых классических асимметричных криптоалгоритмов, что делает крайне актуальной задачу перехода с текущих асимметричных криптографических алгоритмов на постквантовые алгоритмы, стойкие к криптоанализу с использованием квантовых вычислений. Усугубляющим данную проблему фактором также является распространенность в настоящее время метода HNDL (Harvest Now, Decrypt Later – «Собери сейчас, расшифруй позже»), состоящего в сборе и хранении злоумышленниками зашифрованных современными криптоалгоритмами данных (предположительно, имеющих ценность) в надежде на относительно скорое появление квантовых компьютеров и возможность расшифрования собранных данных с их помощью.

Одним из ответов на потенциальную угрозу асимметричной криптографии со стороны квантовых компьютеров явился конкурс Национального института стандартов и технологий США (NIST – National Institute of Standards and Technology) по выбору алгоритмов электронной подписи (ЭП) и инкапсуляции ключей (KEM – Key Encapsulation Mechanism) для стандартизации[2]. Промежуточным результатом конкурса стал выход в 2024 г. трех стандартов на постквантовые криптоалгоритмы:

- FIPS (Federal Information Processing Standard – Федеральный стандарт обработки информации) 203[3] – на алгоритм KEM;
- FIPS 204[4] и 205[5] – на алгоритмы ЭП (со значительно различающимися между собой характеристиками).

1 Панасенко Сергей Петрович, кандидат технических наук, МСР, АО «Актив-софт», Москва, ORCID 0000-0001-6752-5117. E-mail: panasenko@guardant.ru
2 Post-Quantum Cryptography. https://csrc.nist.gov/pqc-standardization.
3 FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. https://doi.org/10.6028/NIST.FIPS.203.
4 FIPS 204. Module-Lattice-Based Digital Signature Standard. https://doi.org/10.6028/NIST.FIPS.204.
5 FIPS 205. Stateless Hash-Based Digital Signature Standard. https://doi.org/10.6028/NIST.FIPS.205.

Таблица 1.

Назначение основных параметров алгоритма SLH-DSA

Параметр	Стандартные значения	Назначение
n	16, 24, 32	Размер в байтах подписываемого хеш-кода и элементов ключей и подписи схемы WOTS+
d	7, 8, 17, 22	Количество уровней деревьев XMSS в гипердереве
h'	3, 4, 8, 9	Высота (количество уровней узлов/листьев) дерева XMSS
a	6, 8, 9, 12, 14	Количество элементов дерева схемы FORS
k	14, 17, 22, 33, 35	Размер элемента дерева схемы FORS в битах

Одной из явных проблем перехода на постквантовые криптоалгоритмы можно считать достаточно высокую (а в ряде случаев, например, в части стандартизованного в FIPS 205 алгоритма SLH-DSA (Stateless Hash-Based Digital Signature Algorithm – алгоритм электронной подписи на основе хеширования без сохранения состояния) – очень высокую) ресурсоемкость постквантовых криптоалгоритмов, включая стандартизованные, тогда как одно из востребованных потенциальных применений таких алгоритмов предполагает их реализацию в устройствах с ограниченными вычислительными ресурсами.

В качестве примера таких применений рассмотрим смарт-карты, представляющие собой защищенные микроэлектронные устройства (в общем случае, с ограниченными вычислительными ресурсами), обычно обладающие криптографическими возможностями, включая вычисление ЭП и выполнение протоколов аутентификации.

В данной работе проводится анализ применимости алгоритма SLH-DSA в смарт-картах, прежде всего, с точки зрения значительно увеличенных размеров его ЭП, и формулируются предложения по модификации стандартного протокола взаимодействия со смарт-картами с целью его адаптации под основные характеристики данного алгоритма.

Основные свойства алгоритма SLH-DSA приведены в разделе 1. Раздел 2 посвящен описанию основных стандартных протоколов информационного обмена между смарт-картами и считывателями, включая основные команды для использования криптографических возможностей смарт-карт в части ЭП. В разделе 3 сопоставляются характеристики алгоритма SLH-DSA и высвечиваются проблемные моменты при его применении с точки зрения протоколов обмена, описанных в разделе 2. Рекомендации по модификации данных протоколов для их адаптации к характеристикам постквантовых алгоритмов ЭП, включая SLH-DSA, даются в разделе 4.

1. Алгоритм SLH-DSA

SLH-DSA основывается на концепции применения одноразовых электронных подписей, в качестве которых используются модифицированная одноразовая электронная подпись Винтерница WOTS+ (Winternitz One Time Signature) [4] и схема электронной подписи с ограниченным количеством применений FORS (Forest of Random Subsets) [5] совместно с многоуровневой древовидной структурой расширенной одноразовой подписи Меркля XMSS (Extended Merkle Signature Scheme) [6]. Определяющий данный алгоритм стандарт FIPS 205 основан на проанализированном в рамках вышеописанного конкурса NIST алгоритме ЭП SPHINCS+ [5] с рядом изменений относительно оригинального алгоритма.

Алгоритм SLH-DSA является параметризуемым и имеет несколько вариантов с фиксированными параметрами, а также подварианты с детерминиро-

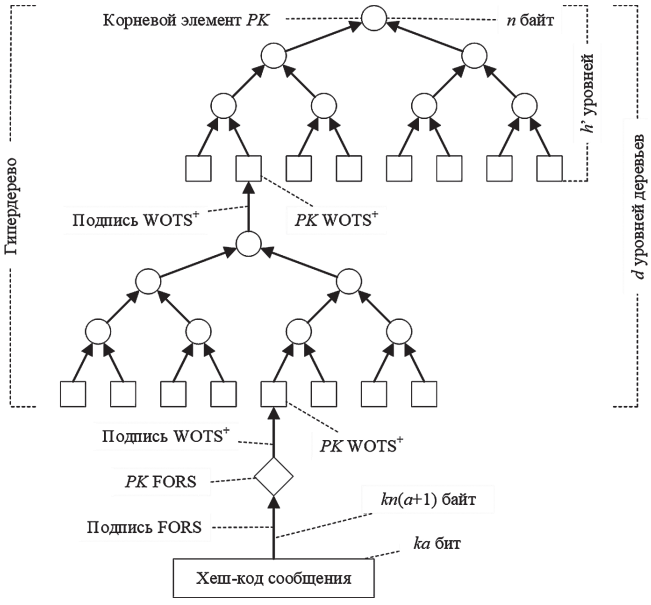

Рис. 1. Упрощенная схема структуры данных алгоритма SLH-DSA

ванным вычислением ЭП и с внешним хешированием. Описание параметров алгоритма приведено в табл. 1, а общая структура алгоритма – на рис. 1.

В числе прочего, параметры алгоритма определяют размеры секретного (SK) и открытого (PK) ключей, а также ЭП; зависимость данных размеров от параметров алгоритма приведена в табл. 2.

Таблица 2.

Размеры ключей и ЭП алгоритма SLH-DSA в зависимости от значений параметров

Элемент	Размер в байтах
Секретный ключ	$4n$
Открытый ключ	$2n$
ЭП	$n(1+k(1+a)+d(h'+2n+3))$

FIPS 205 описывает 12 вариантов алгоритма SLH-DSA: по 6 различных наборов параметров для вариантов данного алгоритма, основанных на хеш-функциях с переменным размером выходного значения SHAKE[6] или хеш-функциях семейства SHA-2[7]. Размеры ключей и ЭП стандартных вариантов алгоритма SLH-DSA приведены в табл. 3, где в наименовании варианта указано, какая хеш-функция в нем применяется; дополнительные индексы в названии каждого из вариантов («s» или «f») обозначают направление оптимизации конкретного варианта: с целью ускорения вычисления ЭП («f» от «fast») или с целью уменьшения ее размера («s» от «small»).

6 Определены в FIPS 202. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. http://dx.doi.org/10.6028/NIST.FIPS.202.

7 Определены в FIPS 180-4. Secure Hash Standard (SHS). http://dx.doi.org/10.6028/NIST.FIPS.180-4.

2. Стандартный протокол взаимодействия со смарт-картами

Различные характеристики смарт-карт (от физических параметров до команд прикладного уровня) стандартизованы в семействах стандартов ГОСТ Р ИСО/МЭК 7816 (контактные карты и общие свойства карт различных интерфейсов), 10536, 14443 и 15693 (бесконтактные карты с различной дальностью действия). Общим для смарт-карт различных типов является стандартный протокол логического уровня APDU (Application Protocol Data Unit)[8], краткое описание которого приведено далее.

2.1. Краткое описание протокола

Протокол APDU предполагает взаимодействие считывателя и карты с помощью двух следующих типов информационных пакетов:

- командный запрос C-APDU (Command APDU), направляемый считывателем карте;
- ответ на командный запрос R-APDU (Response APDU), возвращаемый картой считывателю.

Инициатором обмена данными со смарт-картой является считыватель: карта является ведомым устройством и только отвечает на командные запросы, при этом карта в работоспособном состоянии должна обязательно ответить на каждый запрос считывателя.

Команда C-APDU состоит из следующего набора элементов:

- заголовка фиксированного размера, состоящего из четырех однобайтных полей класса (CLA), кода (INS) и параметров команды (P1, P2);
- опциональных полей размера данных команды (Lc) и самих данных (если команда содержит данные);

8 Определен в ГОСТ Р ИСО/МЭК 7816-4-2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

Таблица 3.

Размеры ключей и ЭП стандартных вариантов алгоритма SLH-DSA в байтах

Вариант алгоритма	Размер в байтах		
	Секретный ключ	Открытый ключ	ЭП
SLH-DSA-SHA2-128s SLH-DSA-SHAKE-128s	64	32	7856
SLH-DSA-SHA2-128f SLH-DSA-SHAKE-128f	64	32	17088
SLH-DSA-SHA2-192s SLH-DSA-SHAKE-192s	96	48	16224
SLH-DSA-SHA2-192f SLH-DSA-SHAKE-192f	96	48	35664
SLH-DSA-SHA2-256s SLH-DSA-SHAKE-256s	128	64	29792
SLH-DSA-SHA2-256f SLH-DSA-SHAKE-256f	128	64	49856

- опционального поля максимального размера данных ответа (Le – если команда подразумевает, что в ответе на нее должны быть переданы данные).

Ответ R-APDU содержит следующие элементы:

- опциональное поле данных ответа;
- двухбайтное поле статуса (SW) выполнения команды (SW1, SW2).

2.2 Команды протокола, относящиеся к электронной подписи

Поскольку выполнение криптографических операций является одним из основных назначений смарт-карт, стандартами ГОСТ Р ИСО/МЭК 7816 предусмотрен достаточно широкий набор команд для выполнения криптографических операций; команды, напрямую относящиеся к ЭП, приведены в табл. 4[9].

Таблица 4.

Команды, относящиеся к процедурам ЭП

Команда	Назначение
GENERATE ASYMMETRIC KEY PAIR	Генерация пары асимметричных ключей или запрос открытого ключа сгенерированной ранее пары
PERFORM SECURITY OPERATION, операция COMPUTE DIGITAL SIGNATURE	Вычисление электронной подписи
PERFORM SECURITY OPERATION, операция VERIFY DIGITAL SIGNATURE	Проверка электронной подписи

Помимо этого, процедуры вычисления и проверки ЭП могут быть использованы в некоторых из команд аутентификации, такие команды перечислены в табл. 5[10].

Таблица 5.

Команды аутентификации, в которых могут быть применены процедуры ЭП

Команда	Назначение
INTERNAL AUTHENTICATE	Аутентификация карты терминалом
EXTERNAL AUTHENTICATE	Аутентификация терминала картой
GENERAL AUTHENTICATE	Аутентификация карты терминалом, аутентификация терминала картой или взаимная аутентификация

9 Определены в ГОСТ Р ИСО/МЭК 7816-8-2011. Карты идентификационные. Карты на интегральных схемах. Часть 8. Команды для операций по защите информации.

10 Определены в ГОСТ Р ИСО/МЭК 7816-4-2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

3. Проблемы применения алгоритма SLH-DSA в смарт-картах

Как видно из приведенной выше таблицы 3, размеры ключей алгоритма SLH-DSA являются относительно небольшими, тогда как размеры ЭП превышают размеры ЭП стандартизованных ранее в США алгоритмов ЭП[11] на 1–3 порядка (в зависимости от конкретного варианта алгоритма SLH-DSA и конкретного сравниваемого алгоритма).

Изначально, при формулировке требований к алгоритмам, подаваемым на конкурс по выбору постквантовых алгоритмов ЭП и KEM для последующей стандартизации, NIST определил уровень криптостойкости алгоритма как наиболее значимый фактор для его выбора, тогда как ресурсоемкость алгоритма (выраженная, прежде всего, в размерах ключей, подписи для алгоритма ЭП, шифртекста для KEM и ресурсах, требуемых для выполнения основных процедур алгоритма)[12] также рассматривалась, но как второстепенный по сравнению с криптостойкостью фактор выбора. При этом применимость алгоритмов в устройствах с ограниченными ресурсами при анализе ресурсоемкости алгоритма практически не рассматривалась.

В дальнейшем, при отборе алгоритмов в последующие этапы конкурса NIST четко следовал данной линии: решающим фактором при сравнении алгоритмов была их криптостойкость, важным фактором была диверсификация вычислительно сложных задач, на которых основаны отбираемые алгоритмы, с целью резервирования на случай появления в будущем быстрых методов решения конкретных задач, тогда как ресурсоемкость алгоритмов рассматривалась как менее важный фактор[13]. Аналогичного подхода NIST придерживается и в рамках проходящего сейчас дополнительного конкурса по отбору постквантовых алгоритмов ЭП[14].

Результатом такого подхода явился выбор SPHINCS+ в качестве одного из стандартизуемых алгоритмов, несмотря на значительные размеры ключей и ЭП, а также очень значительную ресурсоемкость данного алгоритма, процедуры которого выполняются, в общем случае, на несколько порядков

11 Определенных в FIPS 186-5. Digital Signature Standard (DSS). https://doi.org/10.6028/NIST.FIPS.186-5.

12 Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

13 См. отчеты NIST: 1) NIST IR 8240. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8240. 2) NIST IR 8309. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8309. 3) NIST IR 8413-upd1. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8413-upd1.

14 См.: 1) Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf. 2) NIST IR 8528. Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8528.

медленнее традиционных стандартных алгоритмов ЭП[15]. Таким образом, реализация алгоритма SLH-DSA в устройствах с ограниченными ресурсами представляет собой весьма сложную задачу, что в той или иной степени свойственно многим из постквантовых алгоритмов ЭП [7].

Возможны различные аспекты ограничений ресурсов смарт-карт, включая:

- ограниченность вычислительных ресурсов микроконтроллера смарт-карты;
- ограниченность энергонезависимой и (особенно) оперативной памяти;
- ограниченность энергопитания смарт-карты;
- ограниченная полоса пропускания канала связи между смарт-картой и считывателем.

При этом существуют относительно высокопроизводительные смарт-карты, которым практически не свойственны первые два из перечисленных выше ограничений; ограниченность энергопитания, прежде всего, характерна для бесконтактных смарт-карт, питающихся за счет наведенного считывателем сигнала, тогда как ограничение полосы пропускания является свойством стандартного протокола обмена.

4. Подходы к реализации обмена данными между смарт-картой и терминалом в части применения алгоритма SLH-DSA

Рассмотрим возможные варианты организации вычисления ЭП смарт-картой и передачи результатов вычислений (в частности, в рамках выполнения операции COMPUTE DIGITAL SIGNATURE команды PERFORM SECURITY OPERATION) от смарт-карты к считывателю с учетом свойственных смарт-картам ограничений.

4.1. Последовательная реализация вычислений и обмена данными

Схема взаимодействия считывателя и смарт-карты при последовательном вычислении ЭП и передаче результатов приведена на рис. 2.

15 Согласно замерам производительности, выполняемым в рамках проекта eBACS: ECRYPT Benchmarking of Cryptographic Systems. https://bench.cr.yp.to.

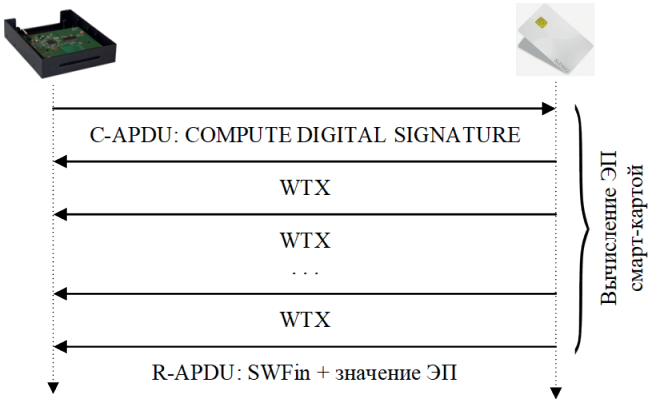

Рис. 2. Схема последовательного взаимодействия

Данная схема основана на следующих предположениях:

- ресурсов смарт-карты (вычислительных ресурсов, оперативной и энергонезависимой памяти) достаточно для размещения программного кода (в случае программной реализации), вычисления ЭП и размещения необходимых для вычисления данных и результатов вычисления;
- смарт-карта поддерживает опциональный расширенный формат C-APDU и R-APDU, который допускает передачу до 2^{16}-1 байт данных команды и до 2^{16} байт данных ответа включительно, в отличие от короткого формата, максимальный размер данных в котором составляет 255 байт; в этом случае даже ЭП максимального размера, предусмотренного алгоритмом SLH-DSA (49856 байт) может быть передана в одном R-APDU; стоит отметить, что расширенный формат R-APDU при его поддержке реализуется путем пофрагментой (не более 256 байт в одном фрагменте) передачи данных нижележащим транспортным протоколом с подтверждением получения каждого фрагмента;
- смарт-карта поддерживает продление времени ожидания ответа на команду от смарт-карты (стандартом[16] предусмотрен таймаут ожидания ответа от карты на команду, который согласовывается в процессе установки соединения и может составлять до нескольких секунд; в случае превышения таймаута терминал имеет право предположить, что карта «зависла», и снять с нее питание) путем направления терминалу запросов WTX (Waiting Time Extension – расширение времени ожидания) на продление времени ожидания; в общем случае, вычисление ЭП с учетом высокой ресурсоемкости алгоритма SLH-DSA может не уложиться в таймаут.

Основным недостатком такого подхода можно считать относительно высокие требования к оперативной памяти, которой должно быть достаточно для хранения вычисленной ЭП целиком до ее отправки в ответе. В совокупности с изложенными выше предположениями о возможностях смарт-карты можно сделать вывод о том, что такой вариант взаимодействия может быть реализован только в смарт-картах, находящихся в верхней части спектра существующих смарт-карт с точки зрения оснащенности ресурсами.

4.2. Пофрагментная передача данных по мере вычисления

Согласно стандарту FIPS 205, ЭП алгоритма SLH-DSA имеет структуру, приведенную в табл. 6.

16 ГОСТ Р ИСО/МЭК 7816-4-2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

Таблица 6.
Структура и размер компонентов ЭП алгоритма SLH-DSA

Компонент	Назначение	Размер в байтах
R	Псевдослучайное значение	n
SIG_{FORS}	ЭП алгоритма FORS	$nk(1+a)$
SIG_{HT}	ЭП гипердерева	$nd(h'+2n+3)$

При этом компоненты ЭП вычисляются последовательно:

- псевдослучайное значение R вычисляется на достаточно раннем этапе в результате хеширования компонента секретного ключа, случайного значения (при его использовании) и подписываемого сообщения;
- затем на основе хеш-кода сообщения и значения R, дополненных компонентами открытого ключа, вычисляется компонент SIG_{FORS}, причем вычисления производятся пофрагментно: выполняется k итераций, в каждой из которых вычисляется $1 + a$ фрагментов по n байт;
- на финальном этапе вычисляется компонент SIG_{HT}, также по-фрагментно: данный компонент состоит из d значений подписи XMSS, каждое из которых имеет размер $n(h'+2n+3)$ и при необходимости может рассматриваться как совокупность фрагментов меньшего размера: сначала – $2n + 3$ фрагментов, затем – h' фрагментов, каждый из них размером по n байт.

Таким образом, вместо последовательного вычисления ЭП и ее передачи выглядит возможным организовать передачу компонентов ЭП по мере их вычисления. Схема обмена данными при таком варианте приведена на рис. 3.

Данная схема по-прежнему предъявляет относительно высокие требования к оперативной памяти для хранения компонентов ЭП (не менее $nd(h'+2n+3)$ байт), а также требует поддержки смарт-картой расширенного формата R-APDU. При этом остается относительно большая вероятность, что вычисление каждого из компонентов не уложится в таймаут, поэтому на рис. 3. приведены запросы WTX для продления времени ожидания ответа.

Показанная на рис. 3 команда GET RESPONSE позволяет получить от карты данные, которые карта готова передать, но по каким-либо причинам не может передать в текущем R-APDU. В случае наличия таких данных об этом сигнализирует специальное значение статуса выполнения текущей команды (обозначено на рисунках как SWPart). Предполагается, что в случае отсутствия ошибок выполнения

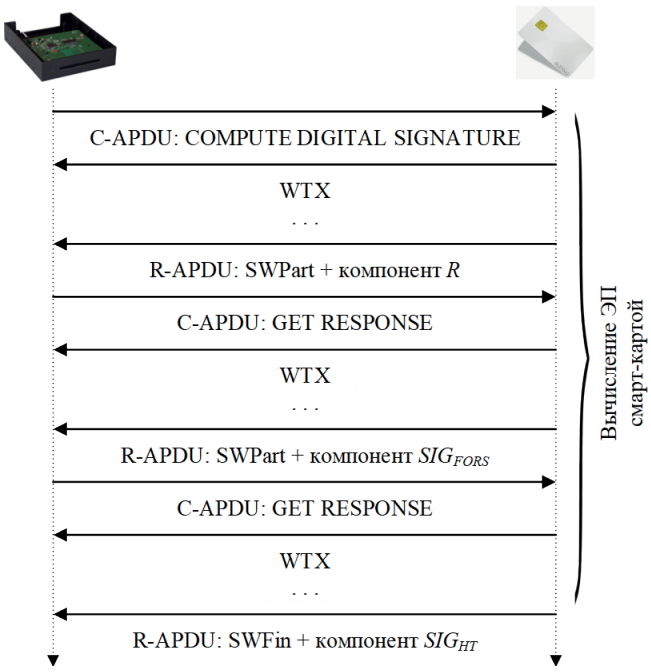

Рис. 3. Покомпонентная передача результатов вычисления

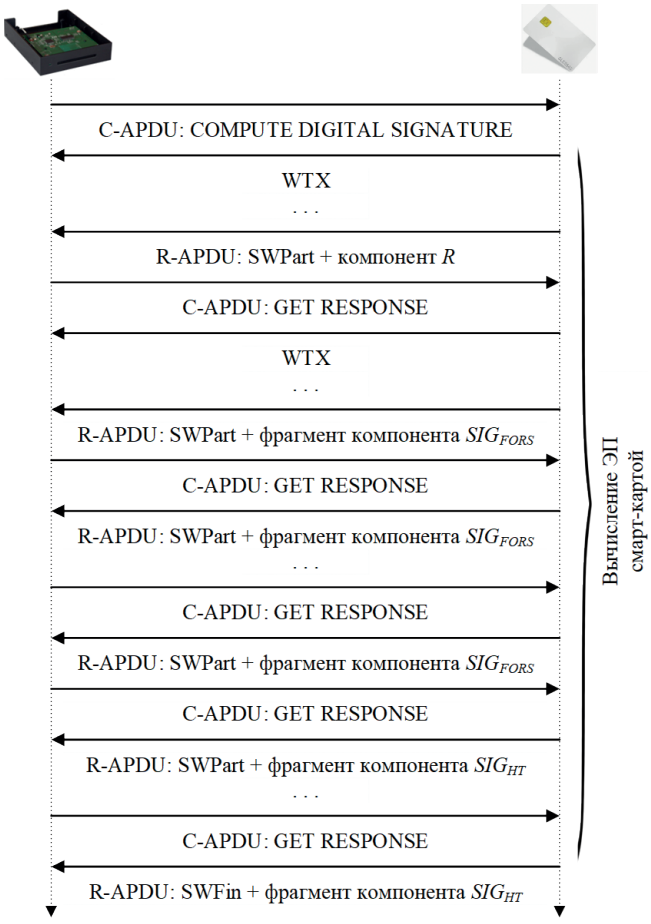

Рис. 4. Пофрагментная передача результатов вычисления

операции при передаче последнего фрагмента передается значение статуса, индицирующее корректное завершение обработки команды[17] (обозначено на рисунках как SWFin). Поскольку команда GET RESPONSE поддерживается не всеми нижележащими транспортными протоколами, вместо нее с тем же эффектом можно использовать цепочки команд C-APDU (устанавливаются определенным битом поля CLA, но поддерживаются не всеми типами смарт-карт) или проприетарные команды, реализующие аналогичный функционал.

Радикального уменьшения требований к оперативной памяти можно добиться дальнейшим разделением компонентов ЭП на n-байтные фрагменты и пофрагментой передачей результатов вычисления ЭП по мере вычисления таких фрагментов (всего $1 + k(1 + a) + d(h' + 2n + 3)$ фрагментов). Схема такого варианта приведена на рис. 4.

Помимо требований к оперативной памяти, данный вариант не требует поддержки картой расширенного формата R-APDU, поскольку n-байтный фрагмент заведомо помещается в 255-байтном блоке данных обязательного для поддержки короткого формата.

В этом случае также может потребоваться наличие запросов WTX в случаях выполнения относительно длительных вычислений перед передачей конкретного фрагмента ЭП. На рис. 4 показаны запросы WTX для таких случаев, которыми являются:

- передача значения R;
- передача первого фрагмента компонента SIG_{FORS}.

Данный вариант взаимодействия также имеет видимые недостатки:

- для эффективного взаимодействия по данной схеме требуется наличие в смарт-карте криптографического сопроцессора (см. далее) или отдельного блока, отвечающего за передачу данных (обычно передача данных управляется центральным процессором (ЦП) смарт-карты), поскольку выполнение генерации ЭП и передачи данных только под управлением ЦП (это справедливо и для описанного ранее варианта с покомпонентной передачей ЭП) по сути является последовательным и, следовательно, применение простой последовательной схемы будет наиболее эффективным для данного случая;
- значительно повышаются накладные расходы в части передачи данных, что, прежде всего, должно проявляться в задержках передачи: для передачи очередного фрагмента ЭП карта должна дождаться получения команды GET RESPONSE; следовательно, данный вариант можно считать эффективным только в том случае, когда время между началом передачи R-APDU с фрагментом данных и завершением получения следующей команды GET RESPONSE не превышает времени вычисления очередного фрагмента ЭП; поскольку расширенный APDU (при его поддержке картой) предполагает схожую пофрагментную передачу данных с квитированием на транспортном уровне, теоретически возможно передавать данные по мере их вычисления в таких фрагментах (путем прямого взаимодействия с транспортным уровнем), что выглядит несколько более эффективным с точки зрения общего времени передачи ЭП;
- важным недостатком можно считать отсутствие поддержки функционала команды GET RESPONSE в ряде протоколов транспортного уровня.

Криптографический сопроцессор смарт-карт при его наличии реализуется в виде отдельного модуля, способного производить вычисления независимо от ЦП (см., в частности, [8]). При этом функциональность такого сопроцессора может быть различной и варьироваться от выполнения конкретных преобразований в рамках алгоритма ЭП до вычисления ЭП целиком; возможности по распараллеливанию вычислений и передачи данных напрямую зависят от полноты реализации в нем процедуры вычисления ЭП. Необходимо отметить, что в бесконтактных смарт-картах параллельные вычисления могут быть ограничены во избежание наведения помех при передаче данных и с целью минимизации энергопотребления.

4.3. Предложения по модификации стандартного протокола обмена данными

С учетом вышесказанного, наиболее эффективным решением выглядела бы возможность передачи n-байтных фрагментов картой по мере их вычисления без ожидания дополнительных запросов от считывателя, что не соответствует протоколу APDU, в рамках которого карта может только отвечать на запросы считывателя определенным образом сформированными пакетами R-APDU. Вариант подобной, схожей с потоковой, передачи данных по мере их формирования стандартом не предусмотрен, но для его поддержки достаточно внесения относительно незначительных изменений в протокол APDU, заключающихся в следующем:

- введение дополнительного значения статуса (обозначим его SWMore), обозначающего тот факт, что в текущем R-APDU передается только часть данных и карта отправит дополнительный ответ с данными по мере их готовности;
- регламентация поведения считывателя при получении такого статуса: считыватель обязан сохранить

17 Команда и значения статуса определены в ГОСТ Р ИСО/МЭК 7816-4-2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

полученные данные (или начать их обработку, если она допустима), продлить период ожидания ответа (аналогично запросу WTX) и ждать получения следующего R-APDU с недостающими данными или их частью.

Схема взаимодействия при реализации данного сценария приведена на рис. 5.

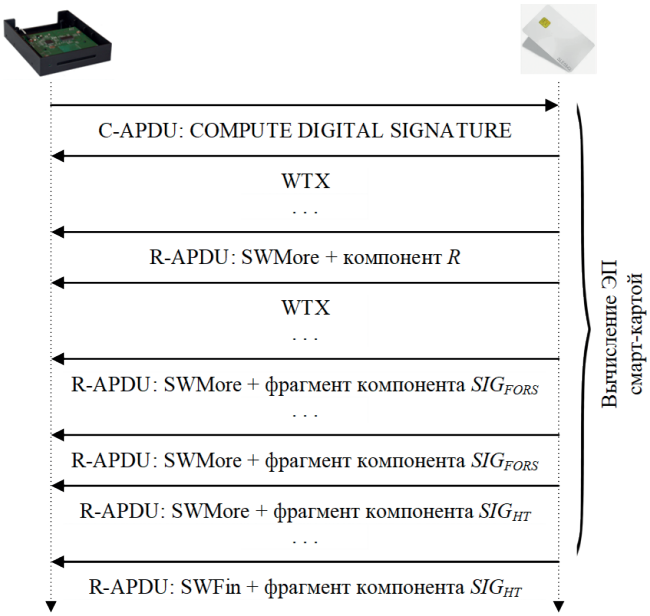

Рис. 5. Потоковая передача результатов вычисления

Данная схема позволит (при наличии у карты технической возможности) параллельно выполнять вычисления ЭП и передачу ее фрагментов сразу после вычисления, не дожидаясь каких-либо дополнительных команд от считывателя, что должно значительно снизить задержки взаимодействия и, таким образом, снизить общее время выполнения команды вычисления ЭП, включая время, требуемое на передачу результата вычисления.

При использовании предлагаемого варианта передачи картой результата вычисления ЭП значительно снижаются требования к карте в части наличия большого объема оперативной памяти и поддержки расширенного формата R-APDU. Тем не менее, поскольку алгоритм SLH-DSA обладает значительными требованиями к вычислительным ресурсам, может быть востребована точная оценка его требований к вычислительным ресурсам смарт-карты, в которой данный алгоритм может быть реализован, с учетом ограниченности времени выполнения его процедур.

Однозначным недостатком предложенной модернизации протокола APDU является предъявление требований к смарт-карте по наличию в ней дополнительных вычислителей, помимо ЦП: криптографического сопроцессора или модуля, управляющего приемом и передачей данных. Распараллеливание передачи данных и вычислений, кроме того, выглядит проблематичным при использовании бесконтактных смарт-карт. Однако необходимо отметить, что невозможность распараллеливания не помешает использованию модернизированного протокола, но сделает его применение неэффективным; в таких случаях могут быть применены стандартные схемы обмена данными, описанные в подразделах 4.1. и 4.2., при условии наличия необходимой поддержки в смарт-карте. Альтернативным вариантом является реализация пофрагментной передачи данных на транспортном уровне.

Еще одним недостатком предложенного подхода является необходимость доработки существующего стандарта, определяющего протокол APDU (стандарт принят достаточно давно, проверен временем и широко используется). Потребуется также модификация программного обеспечения считывателей для внесения предложенной функциональности. Поскольку изменения в протоколе не являются значительными и сохраняют совместимость с выпущенными ранее смарт-картами, модифицированные считыватели должны сохранить возможность взаимодействия как со смарт-картами, соответствующими текущему варианту протокола, так и с новыми смарт-картами с поддержкой предложенных возможностей.

Выводы

Особенности ряда постквантовых алгоритмов ЭП, включая их значительную ресурсоемкость, могут препятствовать применению таких алгоритмов в устройствах с ограниченными ресурсами, в частности, в смарт-картах. Предложенная в данной работе модернизация стандартного протокола APDU позволит снизить требования к смарт-картам, в которых могут быть реализованы ресурсоемкие постквантовые алгоритмы.

Вместе с тем, в ряде смарт-карт применение предложенного протокола не будет эффективным; кроме того, общая ресурсоемкость вычисления ЭП может быть настолько высока, что относительный выигрыш во времени от параллельных вычислений ЭП и передачи данных может быть незначительным.

Следовательно, выглядит востребованной разработка и стандартизация постквантовых криптоалгоритмов с пониженными требованиями к ресурсам для применения в устройствах с ограниченными ресурсами, включая смарт-карты.

Автор выражает благодарность К.Я. Мытнику (АО «НИИМЭ») за крайне ценные замечания по данной работе.

Литература
1. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 1997, 27(5).
2. Chen Z.-Y. et al. Enabling large-scale and high-precision fluid simulations on near-term quantum computers. Computer Methods in Applied Mechanics and Engineering, 2024, 432, Part B, 117428. DOI:10.48550/arXiv.2406.06063.
3. Baumgärtner L. et al. When – and how – to prepare for post-quantum cryptography [Electronic resource]. – URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography#/ (date of treatment: 31.01.2025) – McKinsey Digital – May 4, 2022.
4. Hülsing A. W-OTS+ – Shorter Signatures for Hash-Based Signature Schemes. Report 2017/965 – Cryptology ePrint Archive – TU Darmstadt – 2017.
5. Aumasson J.-P. et al. SPHINCS+. Submission to the NIST post-quantum project, v.3.1 [Electronic resource]. – URL: https://sphincs.org/data/sphincs+-r3.1-specification.pdf (date of treatment: 06.02.2025) – June 10, 2022.
6. Buchmann J., Dahmen E., Hülsing A. XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions. Second Version. Report 2011/484 – Cryptology ePrint Archive – TU Darmstadt – November 26, 2011.
7. Liu T., Ramachandran G., Jurdak R. Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization. arXiv:2401.17538v1 – 31 Jan 2024.
8. Мытник К. Я., Панасенко С. П. Смарт-карты и информационная безопасность / под редакцией д. т. н., профессора В. Ф. Шаньгина. – М.: ДМК Пресс, 2019. – 516 с.

ON THE APPLICABILITY OF THE POST-QUANTUM ELECTRONIC SIGNATURE STANDARD SLH-DSA IN SMART CARDS

Panasenko S. P.[18]

Keywords: *electronic signature, post-quantum cryptography, smart card, APDU protocol, SLH-DSA algorithm.*

The aim of the work: *to analyze the influence of the standard protocol of exchange with smart cards on the applicability of resource-intensive post-quantum algorithms of electronic signature in devices with limited resources using smart cards as an example and to provide recommendations for upgrading the standard protocol based on the analysis results.*

Research methods: *information theory, systems analysis, object-oriented analysis.*

Research results: *various scenarios of interaction with a smart card using the standard protocol of exchange are analyzed using the example of the smart card performing the function of calculating an electronic signature using the SLH-DSA post-quantum algorithm standardized in the USA; as a result of the analysis, limitations of the standard protocol of exchange are shown, directly hindering the applicability of the SLH-DSA algorithm (and algorithms similar in characteristics) in smart cards.*

Scientific novelty: *based on the results of the analysis, a direction of modernization of the standard protocol of exchange with smart cards is proposed for its adaptation to the characteristics of resource-intensive post-quantum algorithms of electronic signature; The proposed protocol upgrade will allow the use of a number of post-quantum cryptographic algorithms in smart cards.*

References
1. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 1997, 27(5).
2. Chen Z.-Y. et al. Enabling large-scale and high-precision fluid simulations on near-term quantum computers. Computer Methods in Applied Mechanics and Engineering, 2024, 432, Part B, 117428.
3. Baumgärtner L. et al. When – and how – to prepare for post-quantum cryptography [Electronic resource]. – URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography#/ (date of treatment: 01/31/2025) – McKinsey Digital – May 4, 2022.
4. Hülsing A. W-OTS+ – Shorter Signatures for Hash-Based Signature Schemes. Report 2017/965 – Cryptology ePrint Archive – TU Darmstadt – 2017.
5. Aumasson J.-P. et al. SPHINCS+. Submission to the NIST post-quantum project, v.3.1 [Electronic resource]. – URL: https://sphincs.org/data/sphincs+-r3.1-specification.pdf (date of treatment: 02/06/2025) – June 10, 2022.
6. Buchmann J., Dahmen E., Hülsing A. XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions. Second Version. Report 2011/484 – Cryptology ePrint Archive – TU Darmstadt – November 26, 2011.
7. Liu T., Ramachandran G., Jurdak R. Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization. arXiv:2401.17538v1 – 31 Jan 2024.
8. Mytnik K. Ya., Panasenko S. P. Smart cards and information security / edited by Doctor of Technical Sciences, Professor V. F. Shan'gin. – M.: DMK Press, 2019. – 516 p.

18 Sergey P. Panasenko, Ph.D., MCP, JSC Aktiv-soft, Moscow, Russia. ORCID 0000-0001-6752-5117. E-mail: panasenko@guardant.ru