РусКрипто

КОМПАНИЯ АКТИВ

Предложения по модификации протокола APDU с целью возможной реализации ряда постквантовых алгоритмов электронной подписи в смарт-картах

Сергей Панасенко

Компания «Актив»
panasenko@guardant.ru

Основные результаты квантового криптоанализа

	Симметричные криптоалгоритмы		Асимметричные криптоалгоритмы		
Классы алгоритмов	Симметричное шифрование	Хеширование	Асимметричное шифрование	Электронная подпись	Вычисление общего ключа
Квантовый криптоанализ	Алгоритм Гровера и его варианты		Алгоритм Шора и его варианты		
Результат криптоанализа	Уменьшение битовой стойкости в два раза		Полное вскрытие		
Метод защиты	Увеличение размеров основных параметров алгоритма		Отсутствует, необходим переход на постквантовые алгоритмы		

Традиционные асимметричные криптоалгоритмы становятся подверженными полному вскрытию в случае появления квантового компьютера с достаточными ресурсами

Пути реагирования на угрозу

#1 Переход на постквантовую криптографию (PQC) сейчас

#2 Модернизация систем, включая переход на PQC, впоследствии

#3 Только усиление традиционных протоколов шифрования

*Baumgärtner L. et al. When – and how – to prepare for post-quantum cryptography. //https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography#/ – McKinsey Digital – May 4, 2022.

Стандартизация постквантовых криптоалгоритмов в США

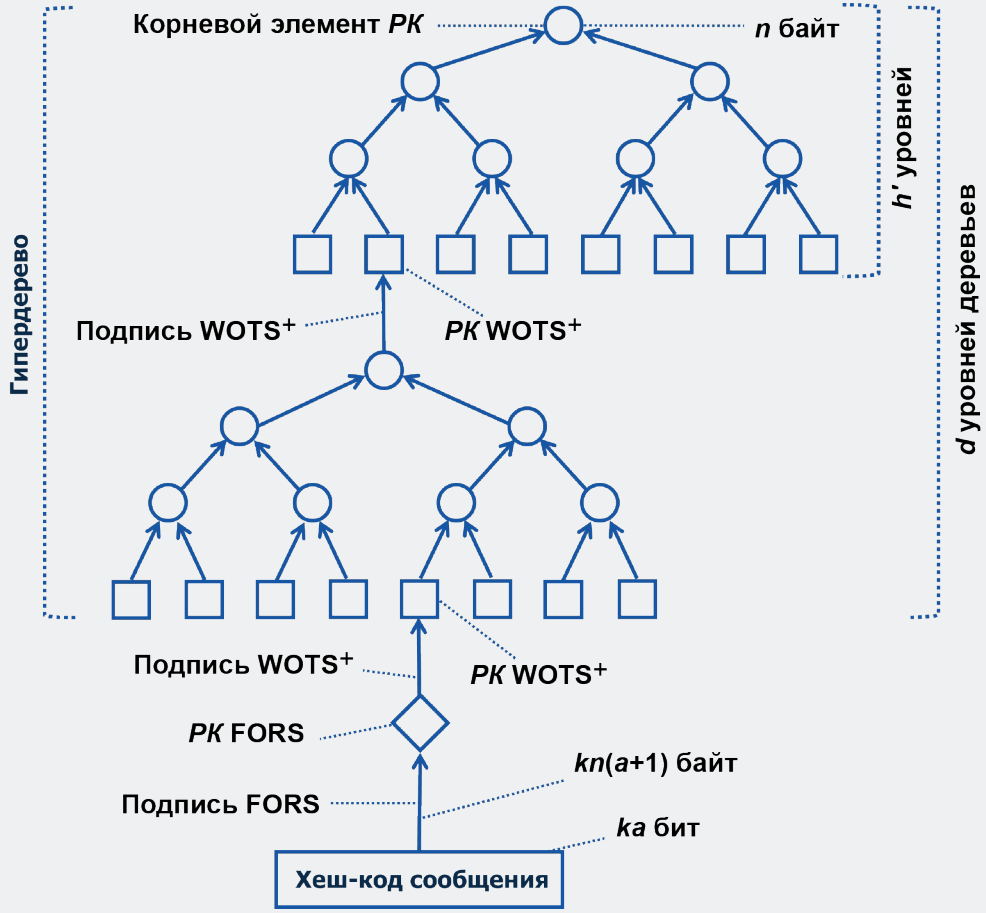
С 2016 г. проводится конкурс NIST по выбору алгоритмов электронной подписи (ЭП) и инкапсуляции ключей (KEM – Key Encapsulation Mechanism) для стандартизации.*

Важнейшим промежуточным результатом конкурса стало принятие трех стандартов США на постквантовые криптоалгоритмы:

- KEM: FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). https://doi.org/10.6028/NIST.FIPS.203.
- ЭП (основной): FIPS 204. Module-Lattice-Based Digital Signature Standard (ML-DSA). https://doi.org/10.6028/NIST.FIPS.204.
- ЭП (резервный): FIPS 205. Stateless Hash-Based Digital Signature Standard (SLH-DSA). https://doi.org/10.6028/NIST.FIPS.205.

* Post-Quantum Cryptography. https://csrc.nist.gov/pqc-standardization.

Алгоритм SLH-DSA



Субалгоритмы:

- FORS (Forest of Random Subsets) – ЭП с ограниченным количеством применений;
- WOTS+ (Winternitz One Time Signature) – одноразовая ЭП;
- XMSS (Extended Merkle Signature Scheme) – одноразовая ЭП, структурирована в виде гипердерева (HT – Hypertree);
- хеш-функции SHA-2 и SHAKE.

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

Основные параметры алгоритма:

- n — главный параметр, определяющий уровень криптостойкости — размер в байтах хеш-кода и элементов ключей
- d, h', a, k — различные параметры субалгоритмов

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

Размеры ключей и ЭП алгоритма SLH-DSA (абсолютные значения)

Вариант алгоритма SLH-DSA	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

Стандартный протокол обмена со смарт-картами

Стандартный протокол логического уровня APDU (Application Protocol Data Unit) является общим для смарт-карт различных типов. *

Предполагает два типа пакетов:

#1 **Командный запрос C-APDU (Command APDU), направляемый считывателем карте:**

- заголовок фиксированного размера, состоящий из четырех однобайтных полей класса (CLA), кода (INS) и параметров команды (P1, P2);
- опциональные поля размера данных команды (Lc) и самих данных;
- опциональное поле максимального размера данных ответа (Le).

#2 **Ответ на командный запрос R-APDU (Response APDU):**

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

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

Команды протокола, относящиеся к ЭП

Процедуры 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

Команды аутентификации:**

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

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

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

Проблемы применения алгоритма SLH-DSA в смарт-картах

- **Высокая ресурсоемкость операций**
- **Большие размеры ЭП**

Смарт-карты обычно обладают ограниченными вычислительными ресурсами.

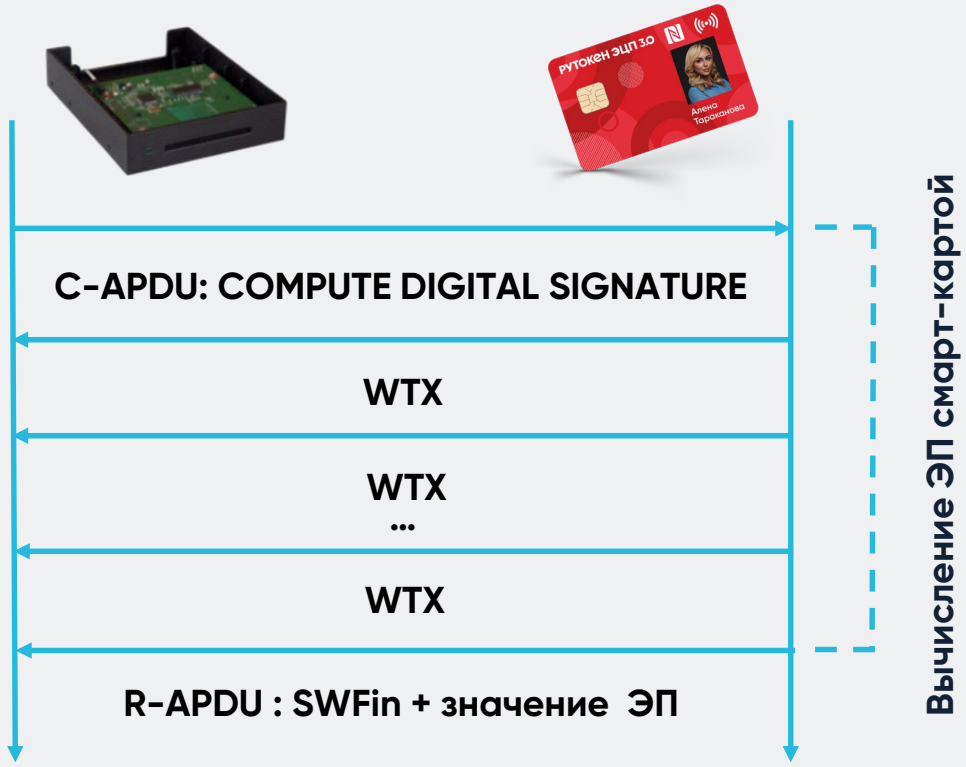
Возможны различные аспекты ограничений ресурсов смарт-карт, включая:

- 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.

Последовательная реализация вычислений и обмена данными

Возможно при следующих условиях:

- достаточные вычислительные ресурсы;
- достаточный объем оперативной и энергонезависимой памяти;
- поддержка картой расширенного протокола APDU;
- поддержка продления времени ожидания ответа (запросы WTX).



Структура и размер компонентов ЭП алгоритма SLH-DSA

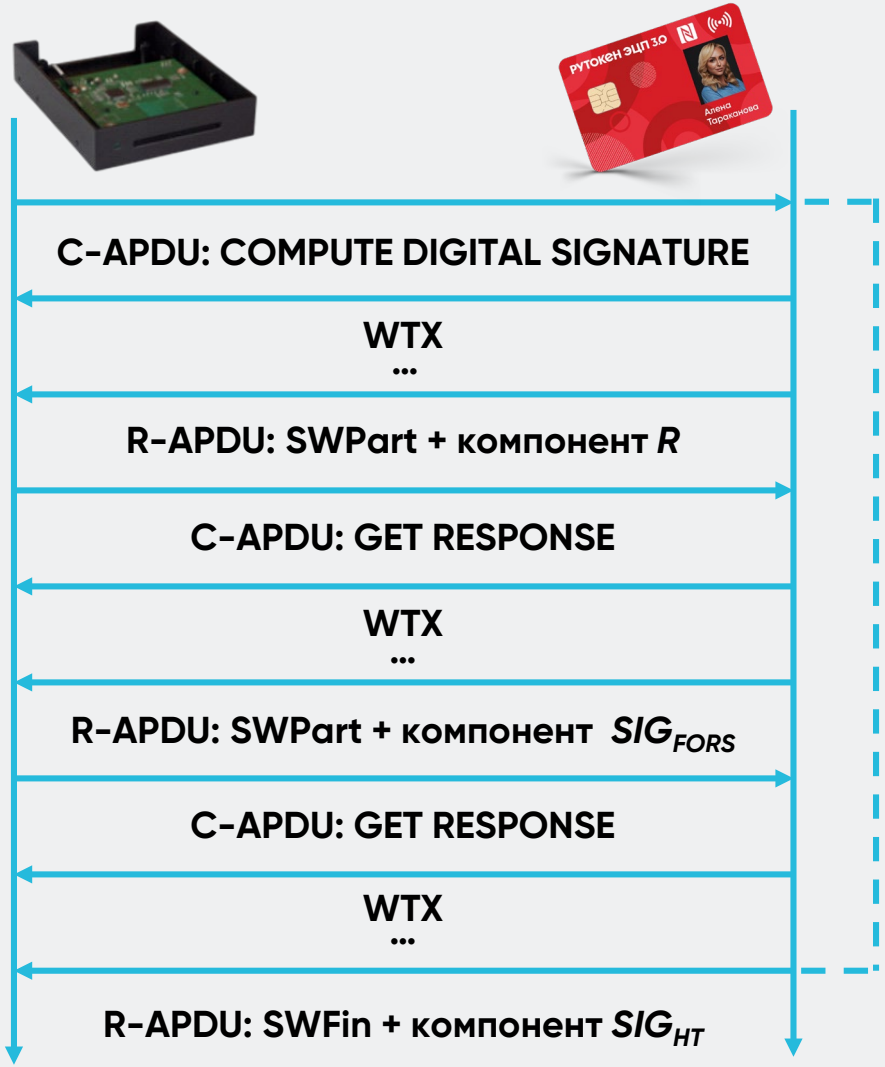
Порядок вычисления соответствует порядку перечисления в таблице:

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

$\boldsymbol{SIG_{FORS}}$ и $\boldsymbol{SIG_{HT}}$ вычисляются фрагментами по n байт: соответственно, $k(1+a)$ и $d(h'+2n+3)$ фрагментов.

Типовые значения n: 16, 24, 32.

Покомпонентная передача по мере вычисления



По-прежнему предъявляет высокие требования:

- к вычислительным ресурсам;
- к оперативной и энергонезависимой памяти;
- требуется поддержка расширенного протокола APDU и запросов WTX.

Недостатки:

- необходим дополнительный вычислитель;
- не все транспортные протоколы поддерживают команду GET RESPONSE.

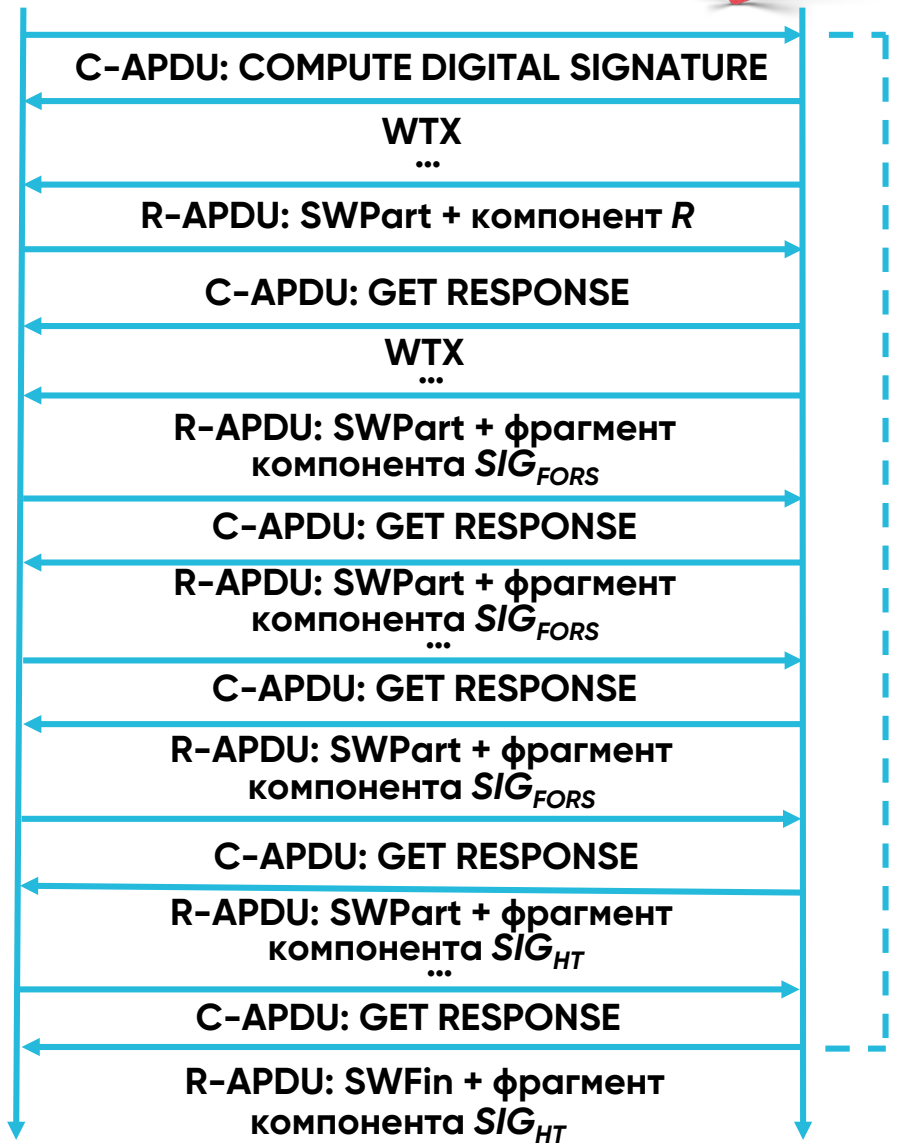
Пофрагментная передача по мере вычисления

Достоинства

- значительно снижены требования к оперативной памяти;
- не требуется поддержка расширенного протокола.

Недостатки

- по-прежнему необходим дополнительный вычислитель и поддержка GET RESPONSE;
- большие накладные расходы на отправку команд/ответов;
- необходимость ожидания команды для отправки фрагмента.



Предложение по модификации стандартного протокола APDU

#1 **Введение дополнительного значения статуса, обозначающего передачу в R-APDU части данных, остальных — по мере готовности**

#2 **Регламентация поведения считывателя при получении такого статуса:**

- сохранение/обработка полученных данных;
- продление периода ожидания ответа (аналогично запросу WTX);
- ожидание получения следующего R-APDU с фрагментом данных.

Преимущества:

- значительное снижение требований к оперативной памяти;
- снижение накладных расходов на передачу данных, отсутствие необходимости ожидания команды для передачи фрагмента данных;
- не требуется поддержка расширенного формата APDU и команды GET RESPONSE.

«Потоковая» пофрагментная передача данных

C-APDU: COMPUTE DIGITAL SIGNATURE

WTX
...

R-APDU: SWMore + компонент *R*

WTX
...

R-APDU: SWMore + фрагмент компонента SIG_{FORS}
...

R-APDU: SWMore + фрагмент компонента SIG_{FORS}

R-APDU: SWMore + фрагмент компонента SIG_{HT}
...

R-APDU : SWFin + фрагмент компонента SIG_{HT}

Вычисление ЭП смарт-картой

Основные недостатки:

- требование наличия дополнительного вычислителя; применение при его отсутствии возможно, но неэффективно;
- необходимость доработки существующего стандарта, определяющего протокол APDU: стандарт принят достаточно давно, проверен временем и широко используется.

Заключение

#1 Высокая ресурсоемкость ряда постквантовых алгоритмов ЭП может препятствовать их применению в смарт-картах. Предложенная модификация стандартного протокола APDU позволит снизить требования к смарт-картам, в которых могут быть реализованы ресурсоемкие постквантовые алгоритмы.

#2 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.

#3 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 данному докладу.

Спасибо за внимание!

КОМПАНИЯ АКТИВ

info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90

Сергей Панасенко

panasenko@guardant.ru