Е. Н. ШКОРКИНА
Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург

КРИПТОГРАФИЧЕСКИЕ НАБОРЫ ПРОТОКОЛА АУТЕНТИФИКАЦИИ НИЗКОРЕСУРСНЫХ УСТРОЙСТВ В ГРАНИЧНОЙ ВЫЧИСЛИТЕЛЬНОЙ АРХИТЕКТУРЕ

Граничные вычисления, позволяющие достичь обработки информации в режиме реального времени, требуют разработки криптографических протоколов, учитывающих новую архитектуру и имеющих в основе алгоритмы, функционирующие в системе с учетом, установленных в системе возможностей нарушителя, и вычислительных характеристик целевых устройств.

В работе описывается протокол аутентификации устройств в граничной архитектуре с установлением ключей управления. Для него выбраны алгоритмы и протоколы, составляющие криптографические наборы двух уровней стойкости (классического и постквантового).

Введение. Обработка и анализ данных в режиме реального времени является неотъемлемой частью современной киберфизической системы. Для обеспечения указанного аспекта были изобретены и развиваются граничные вычисления, предполагающие взаимодействие устройств друг с другом через расположенный в одной локальной сети сервер. Переход к такой вычислительной архитектуре требует разработки новых алгоритмов взаимодействия и механизмов безопасности. Данная работа впервые описывает криптографические наборы протокола аутентификации низкоресурсных устройств двух уровней стойкости.

Аутентификация в граничной вычислительной архитектуре. Иерархическое расположение серверов в логической и физической близости от устройств на границе сети – основной принцип граничных вычислений. При этом данная инфраструктура может быть либо самостоятельной, либо составной частью облачных вычислений, выполняющей предварительную обработку информации перед передачей в облако и принимающей решения для таких задач, как аутентификация. Новые модели взаимодействия предполагают выполнение операций между двумя устройствами или между устройством и облачным сервером только через граничный сервер. Протокол аутентификации, представленный в работе [1], позволяет аутентифицировать одно устройство (управляющее) на другом (управляемом) через граничный сервер (рис. 1). В данной работе рассматривается его модифицированная версия с установлением ключей аутентифицированного управления.

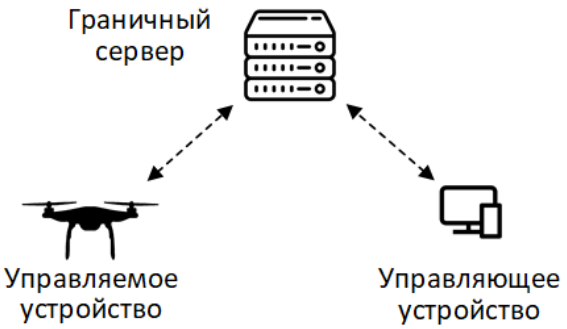

Рис. 1. Модель взаимодействия устройств протокола аутентификации в граничной вычислительной архитектуре

Протокол состоит из двух этапов: сначала выполняется инициализация, а затем аутентификация с установлением ключей управления.

Инициализация. На данном этапе выполняется генерация доверенной стороной подписи $Sign_{ES}$ для идентификационных данных ID_{ES} граничного сервера, а также предварительное

распределение симметричного ключа аутентификации K_{auth} в управляющее и управляемое устройства.

Аутентификация с установлением ключей управления. Протокол состоит из следующих шагов:

1. Управляющее устройство инициирует выполнение протокола аутентификации путем отправки серверу сертификатов открытых ключей шифрования и подписи, содержащих сами ключи $\langle Pk_{Dev_1}^{Enc}, Pk_{Dev_1}^{Sign}\rangle$.
2. При успешной проверке полученных сертификатов граничный сервер формирует и отправляет управляющему устройству шифрограмму вида

$$E_{Pk_{Dev_1}^{Enc}}(Sign_{ES} \oplus r \| r), \tag{1}$$

в которой r – случайное число, длина которого совпадает с длиной подписи $Sign_{ES}$, $\oplus$ – операция побитового сложения по модулю 2.

3. Устройство расшифровывает полученное значение с использованием своего закрытого ключа и проверяет подпись $Sign_{ES}$. Если подпись корректна, то значение $Sign_{ES} \oplus r$ сохраняется как ключ взаимодействия с граничным сервером. Далее формируется и отправляется серверу значение

$$E_{auth}^{sym}(Sign_{ES} \oplus r, K_{auth}), \tag{2}$$

представляющее собой результат применения алгоритма аутентифицированного шифрования к открытым данным K_{auth} на ключе $Sign_{ES} \oplus r$.

4. Граничный сервер получает и расшифровывает K_{auth} с проверкой имитовставки. При успешной проверке значение $Sign_{ES} \oplus r$ сохраняется как ключ алгоритма шифрования для взаимодействия с данным устройством. Далее на ключе K_{auth} формируется шифрограмма,

$$E_{K_{auth}}^{sym}(Sign_{ES} \oplus q \| q\ ), \tag{3}$$

отправляемая управляемому устройству вместе с открытым ключом подписи $Pk_{Dev_1}^{Sign}$.

5. Управляемое устройство расшифровывает полученное зашифрованное значение с помощью ключа K_{auth} и проверяет подпись $Sign_{ES}$. При успешном завершении аутентификация выполнена. Значение $Sign_{ES} \oplus q$ сохраняется в качестве ключа алгоритма расшифрования сообщений, полученных от сервера, а $Pk_{Dev_1}^{Sign}$ – в качестве ключа проверки подписи за управляющее сообщение.

Аутентифицированное управление устройством. Выработанные в результате выполнения протокола ключи $Sign_{ES} \oplus r$ и $Sign_{ES} \oplus q$ используются следующим образом:

1. Управляющее устройство формирует и отправляет граничному серверу:
   - Значение подписи за управляющее сообщение M_{com} с использованием ключа $Sk_{D_1}^{Sign}$:

$$Sign_{M_{com}} = Sign\left(Sk_{Dev_1}^{Sign}, M_{com}\right). \tag{4}$$

   - Шифрограмму с имитовставкой с использованием ключа $Sign_{ES} \oplus r$:

$$E_{auth}^{sym}(Sign_{ES} \oplus r, M_{com} \| Sign_{M_{com}}). \tag{5}$$

2. Граничный сервер расшифровывает полученное значение с проверкой имитовставки. При успешном завершении значение,

$$E_{Sign_{ES} \oplus q}^{sym}(M_{com} \| Sign_{M_{com}}), \tag{6}$$

представляющее собой шифрограмму команды и подписи на ключе $Sign_{ES} \oplus q$, отправляется управляемому устройству.

3. Управляемое устройство расшифровывает полученное значение и проверяет подпись $Sign_{M_{com}}$ за полученное сообщение команды M_{com} с использованием открытого ключа подписи, полученного в результате выполнения протокола аутентификации. Если успешно, то команда выполняется.

Криптографические наборы протокола. Криптографические алгоритмы, определенные в протоколе аутентификации, должны быть выполнимы за разумное время без потери актуальности передаваемой информации на устройствах. При этом выбор множества, с использованием которого будет функционировать протокол аутентификации, должен быть сделан на основе модели угроз системы. Если возможность выполнения нарушителем эффективного квантового криптоанализа не учитывается, целесообразно использовать набор протоколов классического уровня стойкости, в противном случае – постквантового.

Среди асимметричных алгоритмов классического уровня стойкости целесообразно выбирать протоколы на эллиптических кривых, превосходящие криптосистемы на основе модулярной арифметики, во-первых, по быстродействию при аппаратной и программной реализации, а во-вторых, по уровню защищенности в расчете на один бит ключа. Для асимметричного шифрования и цифровой подписи в таком случае следует выбрать соответствующие схемы Эль-Гамаля. Алгоритм симметричного шифрования и аутентифицированного шифрования должен быть подобран на основе результатов функционирования блочного шифра на целевой аппаратной платформе, среди которых должны исследоваться низкоресурсные алгоритмы стандарта ISO/IEC 29192–2:2019, алгоритмы ГОСТ Р 34.12–2018, а также AES-128. Предлагаемый криптографический набор протокола аутентификации классического уровня стойкости приведен в табл. 1.

Таблица 1

Криптографический набор классического уровня стойкости

Обозначение	Тип	Алгоритмы классического уровня стойкости
E / D	Асимметричное зашифрование / расшифрование	Схема шифрования Эль-Гамаля на эллиптических кривых
E^{sym} / D^{sym}	Симметричное зашифрование / расшифрование	Блочной шифр PRESENT, «Магма», либо AES-128 в режиме счетчика (CTR)
E^{sym}_{auth} / D^{sym}_{auth}	Симметричное зашифрование / расшифрование с имитозащитой	Режимы аутентифицированного шифрования: режим MGM с использованием блочного шифра «Магма», либо режим GCM блочного шифра AES-128 [7]
$Sign$ () / $Verify$()	Формирование/ проверка цифровой подписи	Схема подписи Эль-Гамаля на эллиптических кривых

Криптографический набор постквантового уровня стойкости должен содержать асимметричные схемы, безопасность которых основана на математической задаче, являющейся предположительно стойкой к квантовому криптоанализу. По результатам конкурса NIST [2], для цифровой подписи рекомендован к использованию алгоритм CRYSTALS-Dilithium, а для инкапсуляции ключа – алгоритм CRYSTALS-Kyber, безопасность которых основана на сложных вычислительных задачах теории решеток. Алгоритмы показали хорошие результаты, в том числе при реализации на низкоресурсных микроконтроллерах семейств ARM Cortex-M3 и ARM Cortex-M4 [3, 4]. Их использование в протоколе аутентификации (рис. 2) предполагает на шаге 1 передачу вместо открытого ключа шифрования соответствующего ключа инкапсуляции $Pk^{Exp}_{Dev_1}$, а также выработку на шаге 2 по алгоритму $Encaps()$ общего ключа K, имеющего шифртекст c. Далее формируется шифрограмма $E^{sym}_K(Sign_{ES} \oplus r \| r)$ и передается вместе с шифртекстом (шаги 3–4). Для получения управляющим устройством общего ключа выполняется алгоритм $Decaps()$. Схема взаимодействия граничного сервера и управляемого устройства остается без изменений.

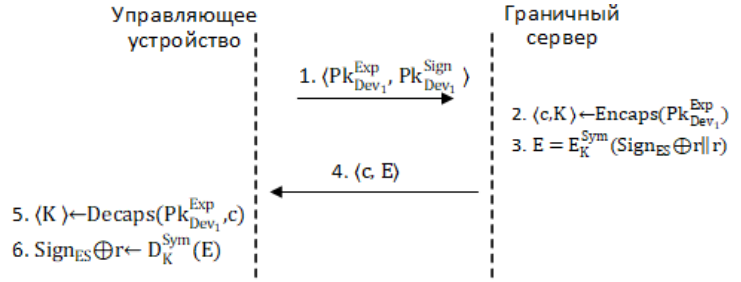

Рис. 2. Внедрение постквантового алгоритма инкапсуляции ключа в протокол аутентификации

С целью сохранения достаточной стойкости к методу криптоанализа с использованием алгоритма Гровера в качестве блочного шифра алгоритмов E^{sym} и E^{sym}_{auth}, необходимо выбирать тот, который имеет длину ключа не менее 256 бит. Предлагаемый криптографический набор протокола аутентификации постквантового уровня стойкости приведен в табл. 2.

Таблица 2

Криптографический набор постквантового уровня стойкости

Обозначение	Тип алгоритма	Алгоритмы постквантового уровня стойкости
$Encaps()$ / $Decaps()$	Выработка общего ключа	CRYSTALS-Kyber
$Sign\ ()$ / $Verify()$	Формирование/ проверка цифровой подписи	CRYSTALS-Dilithium
E^{sym}_{auth} / D^{sym}_{auth}	Симметричное зашифрование / расшифрование с имитозащитой	Режимы аутентифицированного шифрования: режим MGM с использованием блочного шифра «Кузнечик» или режим GCM блочного шифра AES-256
E^{sym} / D^{sym}	Симметричное зашифрование / расшифрование	Блочный шифр «Кузнечик» или AES-256 в режиме счетчика (CTR)

Заключение. Обработка информации с помощью граничных вычислений позволяет функционировать информационным системам в режиме реального времени за счет физической близости серверов к устройствам. Разработанный для данной архитектуры протокол аутентификации с распределением ключей на основе одного из двух криптографических наборов обеспечивает безопасное управление низкоресурсными устройствами.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90110.

ЛИТЕРАТУРА

1. **Aleksandrova E.B., Oblogina A.Y., Shkorkina E.N.** Authentication of Control Devices in the Internet of Things with the Architecture of Edge Computing. *Automatic Control and Computer Sciences*. 2021. V. 55. №. 8. P. 1087–1091.
2. **NIST Announces First Four Quantum-Resistant Cryptographic Algorithms** [Электронный ресурс]. 2022. URL: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (дата обращения 10.07.2022).
3. **Greconici D.O.C., Kannwischer M.J., Sprenkels D.** Compact dilithium implementations on Cortex-M3 and Cortex-M4. *IACR Transactions on Cryptographic Hardware and Embedded Systems*. 2021. P. 1–24.
4. **Botros L., Kannwischer M.J., Schwabe P.** Memory-efficient high-speed implementation of Kyber on Cortex-M4. *International Conference on Cryptology in Africa*. Springer, Cham, 2019. P. 209–228.

E.N.Shkorkina, (Peter the Great St. Petersburg Polytechnic University, Saint Petersburg)

Cryptographic suites for intelligent electronic devices authentication protocol in edge environment

Computations that allow real-time processing of information require the development of cryptographic protocols that consider the new architecture. They should also be based on algorithms that operate in the system, taking into account the capabilities of the intruder and the computing characteristics of the target devices.
The paper describes the device authentication protocol in the edge architecture with the establishment of control keys. For it, algorithms and protocols were selected that constitute cryptographic sets of two security levels (classical and post-quantum).

Авторы готовы представить текст на английском языке для сборника материалов мультиконференции, который будет подан для индексирования в Scopus