Е. Б. АЛЕКСАНДРОВА, Э. А. КРАШЕНИННИКОВ, А. В. ЯРМАК
Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург

СХЕМА КРИПТОГРАФИЧЕСКОГО КОНТРОЛЯ ДОСТУПА К ДАННЫМ ОБЛАЧНОГО ХРАНИЛИЩА НА ОСНОВЕ ИЗОГЕНИЙ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

В рамках доклада представлена схема SIDH-DAC, обеспечивающая защиту от несанкционированного доступа к данным облачного хранилища в условиях недоверенного провайдера облачных услуг. В качестве основы для разработанной схемы была выбрана Crypt-DAC. Особенности используемого математического аппарата изогений эллиптических кривых позволили модифицировать процедуры шифрования и аутентификации. Результаты тестирования программного прототипа показывают, что скорость операций в случае введенных оптимизаций увеличилась в 1,5 – 2,5 раза.

Введение. В настоящее время облачные сервисы представляют собой наиболее распространенный способ хранения большого объема информации, что обусловлено отсутствием необходимости развертывания и обслуживания собственной инфраструктуры, меньшими затратами на персонал и ресурсы, возможностью обеспечения быстрого доступа к данным с различных устройств. Провайдеры облачных ресурсов, как правило, предоставляют традиционные инструменты по контролю доступа к информации. Такие программные решения функционируют на доверенном сервере, который хранит данные в открытом виде и по входящему запросу предоставляет информацию пользователю. Однако в случае недоверенного облачного провайдера или компрометации сервера возникает угроза несанкционированного доступа к данным.

Для решения указанной проблемы предлагается схема, обеспечивающая защиту от несанкционированного доступа к данным с использованием криптографических алгоритмов и протоколов. К достоинствам данной схемы можно отнести совместимость с любой классической моделью контроля доступа, хранение данных в облаке в зашифрованным виде, независимость от архитектуры файловой системы серверов облачного хранилища [1]. Безопасность обусловлена сложностью решения задачи поиска изогений эллиптических кривых.

Обоснование выбора основной модели. Среди исследованных классических моделей контроля доступа одновременно гибкостью и масштабируемостью обладает ролевая модель доступа. Кроме того, в схеме криптографического контроля доступа должны поддерживаться функции добавления субъектов (пользователей), ролей, объектов (файлов), назначения ролей пользователя, разрешений ролям, исключения пользователей из ролей, отмены назначенных разрешений.

Среди подходов к криптографическому контролю доступа в облаке выделяют широковещательное шифрование, шифрование на основе атрибутов и гибридное шифрование [2]. Для реализации последнего может быть использована готовая криптосистема с открытым ключом на изогениях, например, SIDH (Supersingular Isogeny Diffie-Hellman) [3], поэтому именно гибридный подход стал основой для разрабатываемой схемы.

Результаты сравнительного анализа схем криптографического контроля доступа [4–7] представлены в таблице. Несмотря на то, что в схеме IBBE-SGX [6] учтена угроза со стороны администратора, защита от неё осуществляется с использованием аппаратной технологии Intel SGX, что накладывает ограничения на аппаратную составляющую. Таким образом, среди рассмотренных схем криптографического контроля доступа можно выделить две конструкции на основе ролей, использующие гибридное шифрование: HCAC-HER [4] и Crypt-DAC [5]. В схеме HCAC-EHR не рассматривается угроза, исходящая от пользователей, права которых были отозваны, поэтому в качестве основы разрабатываемой схемы контроля доступа на основе задачи поиска изогений была выбрана Crypt-DAC.

Предлагаемая схема криптографического контроля доступа. В предлагаемой схеме в облачном хранилище в зашифрованном виде размещаются файлы, а также политика безопасности, управление которой осуществляет администратор. Выделяются следующие сущности: пользователи (U), роли (R), файлы (F), таблица FK (FileKeys), связывающая роли и файлы, и

таблица RK (RoleKeys), ассоциирующая пользователи и роли. Для каждого пользователя и роли введена пара открытый/закрытый ключ.

Таблица

Сравнительный анализ схем криптографического контроля доступа

Схема		HCAC-HER [4]	Crypt-DAC [5]	IBBE-SGX [6]	C-ABAC [7]
Основная модель		На основе ролей, избирательный	На основе ролей	На основе ролей	Мандатный, избирательный
Криптографическая модель		Гибридная	Гибридная	Широковеща-тельная	На основе атрибу-тов
Угрозы	Внешний злоумышлен-ник	Низкий уровень опасности	Низкий уровень опасности	Низкий уровень опасности	Низкий уровень опасности
	Администратор	Средний уровень опасности	Средний уровень опасности	Низкий уровень опасности	Средний уровень опасности
	Облачный провайдер	Низкий уровень опасности	Низкий уровень опасности	Низкий уровень опасности	Низкий уровень опасности
	Отозванный пользователь	Высокий уровень опасности	Низкий уровень опасности	Низкий уровень опасности	Средний уровень опасности
Дополнительные технологии		Индексация	Ротация ключей	Intel SGX	Атрибуты разных типов

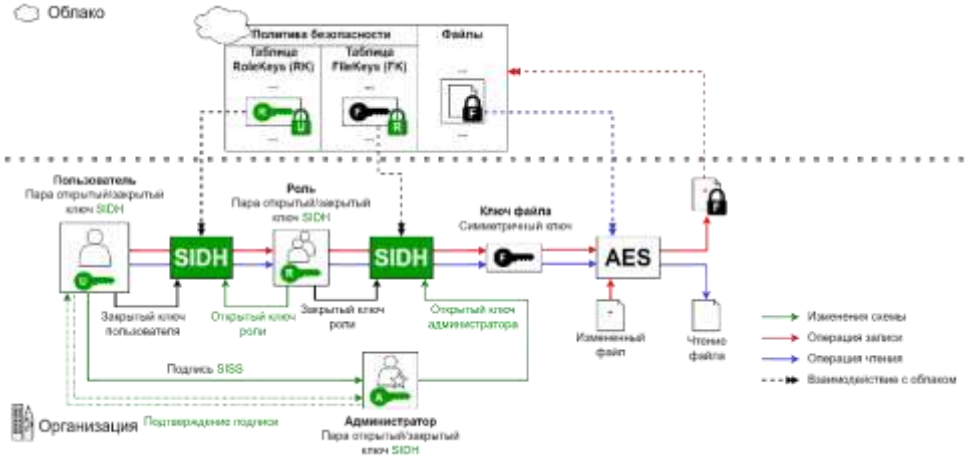

Рис. 1. Схема SIDH-DAC

В схеме Crypt-DAC при операции чтения файла пользователь сначала загружает запись из таблицы RK, в которой хранятся зашифрованные ключи роли. Расшифровать данную запись он может с помощью своего закрытого ключа RSA. Далее пользователь загружает зашифрованный ключ файла из таблицы FK и расшифровывает с использованием полученного ключа роли. Затем он может загрузить, расшифровать и прочесть сам файл. При операции записи пользователь зашифровывает измененный файл, загружает его в облако, а затем отправляет подпись администратору для подтверждения изменений. В предлагаемой схеме SIDH-DAC (Supersingular Isogeny Diffie–Hellman Dynamic Access Control, рис. 1) вместо криптосистемы RSA используется схема шифрования на основе SIDH. Кроме того, введены следующие изменения: для расшифрования данных таблицы RK необходимо использовать закрытый ключ пользователя и открытый ключ роли, а для таблицы FK – закрытый ключ роли и открытый ключ администратора. В качестве протокола электронной цифровой подписи использовалась неоспоримая подпись на изогениях [8], подразумевающая интерактивное взаимодействие с подписывающим.

Модификация схемы. В целях оптимизации предложенной схемы, для ускорения операции записи, была разработана схема Simplified SIDH-DAC (S-SIDH-DAC), основная идея которой заключается в том, что для шифрования в таблице FK и аутентификации используется кривая E'_r, которая известна только администратору и участникам роли. Кривая $E'_r = E_0/\langle nP_A + mQ_A \rangle$ строится с использованием закрытых показателей n, m, как и кривая $E_r = E_0/\langle nP_B + mQ_B \rangle$,

являющаяся частью открытого ключа, но закрытые показатели применяются к образующим другой подгруппы группы кручения.

Таким образом, ключи шифрования записей в таблице FK формируются с использованием кривой E_r' и хэш-значения от имени файла, а аутентификация во время операции записи осуществляется с использованием кривой E_r' и хэш-значения от измененного файла. Администратор, просмотрев данные аутентификации, может сделать вывод о том, что пользователю известны ключи роли и что пользователь подтверждает внесённые изменения. В результате, используя свойства изогений эллиптических кривых и тот факт, что администратору известен закрытый ключ роли, можно заменить процедуру верификации неоспоримой подписи на проверку знания кривой E_r'.

Программная реализация и результаты тестирования. Прототипы схем SIDH-DAC и S-SIDH-DAC были реализованы в системе компьютерной алгебры SAGEMATH. Оценка трафика производилась путём суммирования объемов данных, необходимых для корректной работы алгоритма через Интернет без учета служебного трафика. Так как в системе SAGEMATH не поддерживается вычисление изогений больших степеней, скорость разработанных прототипов сравнительно невысока и может быть повышена с использованием низкоуровневых оптимизаций. Результаты тестирования представлены на рис. 2.

Рис. 2. Результаты тестирования схем SIDH-DAC и S-SIDH-DAC

В ходе трех тестовых запусков в систему было добавлено 50 пользователей, 5 ролей, 40/20/100 файлов, 50/100/150 записей в таблице FK и 200/100/200 записей в таблице RK. Основное влияние на производительность оказывает количество записей в таблице FK. В среднем скорость S-SIDH-DAC в 1,5–2,5 раза выше, чем SIDH-DAC. Введённая в S-SIDH-DAC оптимизация алгоритма аутентификации повышает производительность примерно в 20 раз.

Заключение. Предложенные в работе схемы SIDH-DAC и S-SIDH-DAC позволяют реализовать контроль доступа на основе ролей даже при ограниченном наборе инструментов, представленных облачным провайдером. Применение шифрования на основе изогений эллиптических кривых обеспечивает безопасность хранения данных в недоверенном облачном хранилище даже при условии появления квантового компьютера достаточно высокой кубитности.

Заметим, что операции изменения политики безопасности в предлагаемых схемах могут выполняться достаточно медленно. При исключении пользователя и лишении прав роли необходимо не только удалить записи из таблиц, но и обновить ключи шифрования всех ранее доступных компонент системы. Данная особенность является ограничением не только разработанных схем, но и схемы Crypt-DAC, которая лежит в их основе. Эту проблему можно решить различными способами в зависимости от требований политики безопасности организации, например, за счет хранения дополнительных ключей и делегирования операций повторного шифрования облачному провайдеру.

Исследование выполнено при финансовой поддержке Минцифры России (грант ИБ) в рамках научного проекта № 12/21-к

ЛИТЕРАТУРА

1. **Kayem A. V. D. M., Akl S. G., Martin P.** Adaptive cryptographic access control. Springer Science & Business Media. 2010. Vol. 48.
2. **Contiu S.** Applied Cryptographic Access Control for Untrusted Cloud Storage. Université de Bordeaux, 2019. 124 p.

3. **Jao D., Feo L. D.** Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. International Workshop on Post-Quantum Cryptography. Springer, Berlin, Heidelberg, 2011. Pp. 19-34.
4. **Chinnasamy P., Deepalakshmi P.** HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. *Journal of Ambient Intelligence and Humanized Computing*. 2022. Vol. 13. №. 2. Pp. 1001-1019.
5. **Qi S., Zheng Y.** Crypt-DAC: cryptographically enforced dynamic access control in the Cloud. *IEEE Transactions on Dependable and Secure Computing*. 2019. Vol. 18. №. 2. С. 765-779.
6. **Contiu S. et al.** IBBE-SGX: Cryptographic group access control using trusted execution environments. *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (DSN). IEEE, 2018. Pp. 207-218.
7. **Zhu Y. et al.** Cryptographic attribute-based access control (ABAC) for secure decision making of dynamic policy with multiauthority attribute tokens. *IEEE Transactions on Reliability*. 2019. Vol. 68. №. 4. Pp. 1330-1346.
8. **Jao D., Soukharev V.** Isogeny-based quantum-resistant undeniable signatures. International Workshop on Post-Quantum Cryptography. Springer, Cham, 2014. Pp. 160-179.

E.B.Aleksandrova, E.A.Krasheninnikov, A.V.Yarmak (Peter the Great St. Petersburg Polytechnic University, Saint-Petersburg)

Isogeny-based scheme of cryptographic access control in the cloud

The paper presents the SIDH-DAC scheme, which ensures security against unauthorized access to cloud storage data. Crypt-DAC was chosen as the basis for the developed scheme. The isogenies' features made it possible to modify the encryption and authentication procedures. The results of software prototype testing show that the speed of operations in the case of the introduced optimizations increased by 1.5–2.5 times.

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