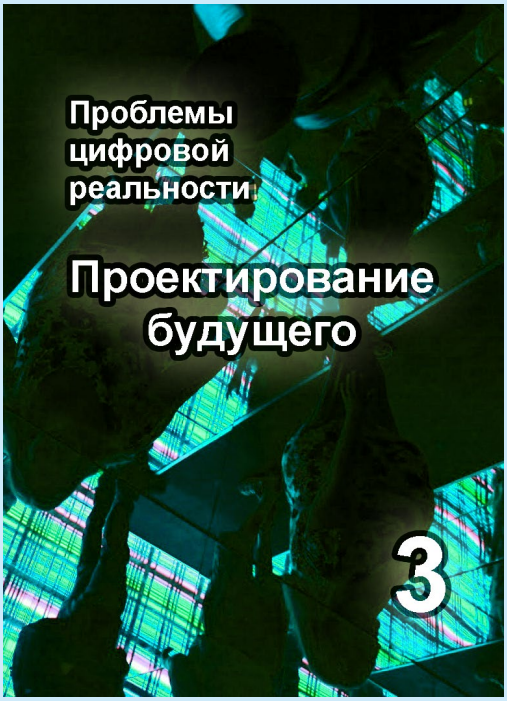
ИПМ им.М.В.Келдыша РАН

Будущее-2020 • Труды конференции



А.Ю. Щербаков

Перспективы современной криптографии

Рекомендуемая форма библиографической ссылки

Щербаков А.Ю. Перспективы современной криптографии // Проектирование будущего. Проблемы цифровой реальности: труды 3-й Международной конференции (6-7 февраля 2020 г., Москва). — М.: ИПМ им. М.В.Келдыша, 2020. — С. 227-233. — https://keldysh.ru/future/2020/20.pdf https://doi.org/10.20948/future-2020-20

Размещено также видео выступления

Перспективы современной криптографии

А.Ю. Щербаков

Центр развития криптовалют и цифровых финансовых активов ВИНИТИ РАН

Аннотация. Рассмотрены основные тренды развития современных криптографических методов защиты информации для платформенных решений цифровых технологий, использующих криптографические механизмы для обеспечения собственной функциональности, проиллюстрирован тезис о том, что трендом развития парадигмы безопасности распределенных недоверенных систем является переход от алгоритмической безопасности к синергии технических и криптографических решений, отказ от «человеческого фактора» в управлении ключами, выработка высококачественных ключей, использование механизма их квантового распределения, отказ от удостоверяющих центров, использование симметричных алгоритмов шифрования. Основным трендом современной криптографии в этих условиях является защита внешнего периметра корпоративного бизнес-процесса, независимого от пользователя, универсальное использование криптографических услуг как внешнего сервиса.

Ключевые слова: шифрование, квантовая криптография, код аутентификации, распределенные реестры, ключи, электронная подпись, обмен ключами, безопасность, шифратор, платформа, HSM (hardware security module) – модуль доверенного хранения ключей, датчик случайных чисел

Prospects for modern cryptography

A.Yu. Shcherbakov

Center for development of cryptocurrencies and digital financial assets VINITI RAS

Abstract. Describes the main trends of development of modern cryptographic methods of information protection for platform solutions of digital technology that uses cryptographic mechanisms to provide its functionality, illustrates the thesis that the development of the paradigm of security of untrusted distributed systems is the transition from algorithmic security to the synergy of technical and cryptographic solutions, the rejection of the “human factor” in the key management, the development of high quality

public key, using the mechanism of the quantum distribution, rejection of CA, use of symmetric encryption algorithms. The main trend of modern cryptography in these conditions is the protection of the external perimeter of the corporate business process, independent of the user, and the universal use of cryptographic services as an external service.

Keywords: encryption, quantum cryptography, authentication code, distributed registries, keys, electronic signature, key exchange, security, encryptor, platform, HSM (hardware security module), random number sensor

1 Введение

Рассматривая эволюцию и стратегии развития современных информационных систем, необходимо отметить, что, в первую очередь, мы явно или неявно пытаемся решить задачу интеграции систем, процессов в этих системах и данных, а также разрешить проблемы распределенности, разомкнутости и недоверенности актуальных информационных систем, которые пришли на смену локальности, замкнутости и доверенности «доинтернетных» компьютерных систем. При этом криптографические механизмы рассматриваются как основные и главные для решения данных проблем.

Надо отметить, что достаточно часто наука и техника, в частности математика, информатика и программирование, исторически развиваются от частного к общему. Например, теория вероятности развивалась от вполне удачных практических методов, обосновываемых реальными статистическими наблюдениями, к аксиоматике, которая появилась почти веком позже.

То же самое мы наблюдаем в криптографии – мы имеем практически действующие инструменты, в первую очередь, достаточно надежные алгоритмы шифрования данных, фиксации и контроля целостности данных, цифровой подписи, решающие проблемы как интеграции распределенных недоверенных информационных систем, так и обеспечения их информационной и инфраструктурной безопасности. Однако теоретическое осмысление архитектур информационных систем и необходимых криптографических методов создания эффективных систем и процессов еще далеко от своей зрелости.

При этом можно констатировать появление принципиально новых методов «квантовой криптографии», когда распределение криптографических ключей происходит путем использования отдельных поляризованных квантов, перехват которых в канале оптической связи невозможен, поскольку меняются свойства квантов.

Квантовые коммуникации, как указано в [1], обеспечивают консистентность данных и самой системы, а значит, «уменьшают» распределенность системы за счет квантово-физических процессов.

2 Перспективы интеграции криптографических механизмов

Посмотрим на проблему интеграции криптографических механизмов с другой стороны – не со стороны механизмов, а со стороны требований.

Современная защищенная платформа с точки зрения ее участников должна обладать следующими априорными свойствами:

1. Обеспечение транзакционных механизмов, т.е. отправление и получение транзакций с гарантиями их доставки и ведение журнала транзакций.
2. Идентификация отправителя/идентификация получателя транзакции.
3. Подтверждение полномочий отправителя / получение полномочий получателя.
4. Определение наличия ресурсов для совершения транзакции.
5. Протоколирование и неотказуемость отправителя/получателя от совершенной (выполненной) транзакции.
6. Наличие возможностей обращения участников к третьей стороне для разрешения возможных конфликтов.
7. Наличие возможностей по контролю за совершением транзакций.
8. Наличие механизмов обеспечения меток времени, обеспечения последовательности транзакций и средств обеспечения информационной безопасности транзакций.

Для выполнения всех этих свойств необходимо использование криптографических методов.

Что принципиально нового дает использование квантового распределения ключей в транзакционной, да и любой другой современной информационной системе?

В первую очередь – переход от алгоритмической защиты (в частности, протоколов работы и регламентов выработки и распределения ключей и функционирования удостоверяющих центров (УЦ)) к технической или физической, когда за безопасность распределения ключей отвечают физические процессы, а за безопасность передачи данных – симметричные криптографические алгоритмы.

Небезопасность обработки ключей с использованием удостоверяющих центров уже стала источником реальных злоумышленных действия [2], что позволяет утверждать, что проблема не только весьма актуальна, но и перешла уже в практическую плоскость.

Однако безопасность распределенных (в смысле розданных пользователям) ключей должна быть обеспечена их корректным хранением. В этом и состоит идея квантового аппаратного модуля безопасности (Quantum HSM, QHSM) – разместить выработанные и распределенные между участниками ключи в физическом хранилище, технически (гальванически или оптически) связанном с устройством квантового распределения ключей и шифрования, при этом хранилище обеспечивает неизвлекаемость ключей из него. Понятие неизвлекаемости

на современном техническом уровне приблизительно можно трактовать так: в хранилище, понимаемом как изолированное техническое устройство, нет возможности прочитать загруженный в него ключ за счет отсутствия программных и технических интерфейсов извлечения ключа во «внешний мир», а также нет возможности извлечения любой информации о нем, существенно раскрывающей содержание ключа, а также отсутствие (в техническом плане) информации о ключе в технических каналах наблюдения (электромагнитном, акустическом, визуальном).

Кроме того, QHSM (или в кириллическом написании – квантовый модуль доверенного хранения ключей, КМДХК) должен обеспечивать выполнение криптографических операций (преобразований) на загруженном в него ключе, а также выработку собственных ключей без их извлечения и выдачу вовне результатов криптографических операций.

Вполне очевидно, что при соблюдении свойств «необратимой или сингулярной» загрузки ключей в QHSM (по аналогии с физической «черной дырой», куда информация и материя попадают безвозвратно) процессы управления ключами осуществляются по их номеру или идентификатору. Кроме того, для хранения идентификаторов вполне можно применять распределенный реестр, а ключи, хранящиеся в QHSM, использовать для верификации данных участников системы, их аутентификации, разрешения споров (например, поскольку квантовые ключи выработаны двумя нодами, то они могут быть использованы для подтверждения транзакции между пользователями).

Ключевым моментом являются механизмы генерации ключей, т.е. корректной работы датчиков случайных чисел и проверки качества случайных последовательностей [3].

Кроме того, в качестве перспективных задач криптографической защиты типовых бизнес-процессов можно сформулировать следующие:

1. Безопасное хранение аутентифицирующей информации пользователей для доступа в различные сервисы.
2. Защита данных в открытых сервисах, включая мессенджеры и открытую почту.

Угроза безопасности в данном случае выглядит следующим образом: пользователь либо небезопасно хранит пароли в доступном мете, либо забывает их, кроме того, использует различные открытые сервисы для передачи служебной информации, что приводит к систематически инцидентам информационной безопасности.

3 Пути решения актуальных задач криптографической защиты

Решение данных задач связано с использованием криптографической защиты (шифрование данных), которая используется для защиты контейнера с паролями, либо для шифрования вложений в открытые почтовые сервисы и мессенджеры.

При этом необходимо помнить о следующих ограничениях:

– грамотное использованием средств криптографической защиты информации (СКЗИ) у пользователя затруднено условиями безопасной эксплуатации и зачастую не может быть реализовано;

– затруднено корректное формирование и хранение ключей на устройстве пользователя;

– зачастую для функционирования СКЗИ необходимо использование удостоверяющих центров, что снижает доступность сервисов и удорожает процесс эксплуатации;

– СКЗИ невозможно установить на пользовательское устройство.

Таким образом, возникает задача разработки СКЗИ в корпоративном периметре, который самостоятельно формирует и хранит ключи по принципу описанной выше технической сингулярности и обеспечивает сервис для пользователя по номеру (идентификатору) ключа после аутентификации пользователя.

При этом требования к аутентификации существенно ниже, чем для хранения ключей. В частности, пароли для доступа могут высылаться на мобильное устройство для каждого сеанса, а также формироваться на основе качественных датчиков случайных чисел.

4 Краткое описание технологии

Пользователь владеет мобильным устройством, имеющим связь с сервером аутентификации и криптографических сервисов (САКС), к которому подключен **модуль доверенного хранения пользовательских ключей (МДХПК).**

МДХПК самостоятельно без участия пользователя формирует при помощи качественного ДСЧ ключи шифрования и хранит их без выдачи во внешнюю среду и выполняет на них функции зашифрования и расшифрования данных.

Пользователю сообщается только идентификатор ключа, на котором производится шифрование.

Аутентификация производится путем присылки на мобильное устройство одноразовых паролей, которые вводятся в программы связи с сервером и используются для реализации протоколов аутентификации.

При необходимости на мобильное устройство может быть передан ключ для создания защищенного сеанса с сервером, закрытый на одноразовом пароле.

Возможен также случай, когда после аутентификации связь с сервером происходит по корпоративной защищенной сети и шифрование и расшифрование информации, переданной от пользователя, происходит внутри МДХПК.

5 Сценарий применения

1. Хранение паролей

Для входа в корпоративные сервисы пользователь запускает приложение, которое производит его аутентификацию и по имени пользователя, которое совпадает или связно с идентификатором его ключа, производит расшифрование контейнера с паролями (хранящимися у пользователя, либо на сервере, что предпочтительнее с точки зрения централизации управления доступом и смены паролей) и автоматически вводит необходимый пароль в нужный сервис, предоставляя пользователю доступ и предусмотренное для него разграничение полномочий.

2. Защита открытой почты или мессенджера

При старте приложения почты или мессенджера автоматически запускается плагин, который производит аутентификацию пользователя и зашифровывает все вложения с учетом адреса (адресов) получателей на ключах получателей, либо на ключах парной связи, которые также принадлежат к данной замкнутой корпоративной системе.

Отправка данных получателю, не входящему в состав корпоративной системы, либо запрещена, либо производится шифрование данных на ключе самого пользователя (для обеспечения архивного хранения данных в почте с возможностью их последующего расшифрования самим пользователем).

Таким образом, оператор почты и внешний нарушитель имеют дело только с закрытыми данными, которые логически не выносятся за периметр безопасности.

Получатели в почте также открывают вложения только на мобильном устройстве после аутентификации с использованием сервисов МДХПК.

6 Выводы

Данная технология позволяет существенно снизить риски нарушения информационной безопасности и не нагружать пользователей неудобными и непривычными им сервисами. Кроме того, корпоративная сеть становится замкнутой и нет необходимости устанавливать СКЗИ на каждое устройство, что позволяет снизить издержки и обеспечить корректную национальную регуляцию в части использования криптографических средств.

Литература

1. *Гриняев С.Н., Правиков Д.И., Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю.* Основные методологические подходы к формированию и обоснованию архитектуры и протокола квантового распределенного реестра // Научно-техническая информация, сер. 2 Информационные процессы и системы. 2020, №1, с.11-18

2. Электронная подпись оставила без квартиры – Коммерсант, 16.05.2019. https://www.kommersant.ru/doc/3969174
3. *Иванов М.А., Чугунков И.В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М: Кудиц-образ, 2003 – 240 с.