МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра оптики и биофотоники

Анализ актуальных методов в средствах криптографической защиты информации

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента магистратуры 2 курса 2223 группы
направления 03.04.02 «Физика»,
профиль «Квантовые технологии»
института физики

Теклина Ильи Александровича

Научный руководитель,
доцент, к.ф.-м.н., _____ П.А. Дьяченко
должность, уч. степень, уч. звание — инициалы, фамилия

Зав. кафедрой,
д.ф.-м.н., профессор _____ В.В. Тучин
должность, уч. степень, уч. звание — инициалы, фамилия

Саратов 2023

Введение

Современные криптографические алгоритмы основаны на фундаментальном процессе факторизации больших целых чисел на их простые значения. Стоит учесть, что современная криптография уязвима как для технологического прогресса вычислительных мощностей, так и для эволюции в математике для быстрого обращения односторонних функций, таких как факторизации больших целых чисел. Решение состоит в том, чтобы внедрить квантовую физику в криптографию. Квантовая криптография является одной из развивающихся тем в области компьютерной индустрии. Данная работа посвящена криптографии в целом и тому, как эта технология приводит к полностью безопасному распределению ключей распределения. Здесь мы рассмотрим слабые стороны современных цифровых криптосистем, фундаментальные концепции квантовой криптографии, реальное применение этой технологии в реальном мире наряду с ее ограничениями, и, наконец, будущее направление, в котором движется криптография, а также работу современных криптопровайдеров.

Основное содержание работы

Криптография с открытым ключом предполагает сложные вычисления, которые выполняются относительно медленно. Они используются для обмена ключами, а не для шифрования больших объемов данных. Например, широко распространенные решения, такие как RSA и схемы согласования ключей Диффи-Хеллмана, обычно используются для распределения симметричных ключей между удаленными сторонами. Однако, поскольку асимметричное шифрование значительно медленнее симметричного, многие учреждения предпочитают использовать гибридный подход, чтобы воспользоваться преимуществами скорости системы общего ключа.

Заключение. Передача и хранение данных в современных реалиях, где данные чрезвычайно важны, должны быть настолько безопасными, насколько это возможно. Эти две традиционные процедуры симметричных ключей и методы открытого доступа (включая RSA, El Gamal, ECC и DSA) находятся под реальной угрозой со стороны квантовых компьютеров (3DES, AES). Создается впечатление, что мы все ближе подходим к созданию полностью целенаправленного всемирного квантового компьютера, который сможет использовать влиятельные квантовые алгоритмы. Результатом этого

технологического развития является полный крах современных безопасных методов открытого ключа, таких как RSA и криптосистемы с эллиптическими кривыми.

Исследования в сфере квантовых технологий все еще продолжаются, чтобы разработать усовершенствованные протоколы и повысить безопасность уже существующих. Но до сих пор все разработанные протоколы являются вариантами протокола BB84. Возможно, будут разрабатываться все новые и новые протоколы, которые будут предоставлять более безопасные и надежные варианты. Появление методов криптографии, не подверженных влиянию квантовых вычислений, является решением этой угрозы.

В связи со стремительным развитием информационных технологий появляется возможность хранить и передавать всё большие объёмы информации. Но это благо имеет и оборотную сторону. Информация становится все более уязвимой по разным причинам:

возрастающие объемы хранимых и передаваемых данных;

расширение круга пользователей, которые имеют право доступа к данным;

усложнение режимов эксплуатации вычислительных систем.

Поэтому все большую важность приобретает проблема защиты информации от несанкционированного доступа при её передаче и хранении.

Выбор двух простых чисел p и q таких, что p не равно q.

Вычисление модуля - произведение p и q: n = p * q. Вычисление функции Эйлера: f = (p - 1) * (q - 1).

Выбор числа E - открытой экспоненты. Это число должно отвечать следующим критериям: оно должно быть простое, оно должно быть меньше f, оно должно быть взаимно простое с f.

Пара {E, n} - открытый ключ.

Вычислить число D, обратное E по модулю f. То есть остаток от деления по модулю f произведения D * E должен быть равен 1:

(D * E) mod f = 1.

Пара {D, n} - закрытый ключ.

Зашифрование:

Пусть A - это исходная информация, которую необходимо зашифровать. Тогда: B = AE (mod n) - зашифрованная информация.

Расшифрование:

Расшифрование зашифрованной информации происходит с помощью закрытого ключа по следующей формуле: A = BD (mod n).

Замечание: необходимым условием корректной работы данного алгоритма является то, что кодируемое сообщение A не должно быть больше числа n.

Обобщенная последовательность действий, которые включает в себя данный алгоритм, продемонстрирована на рисунке 1.

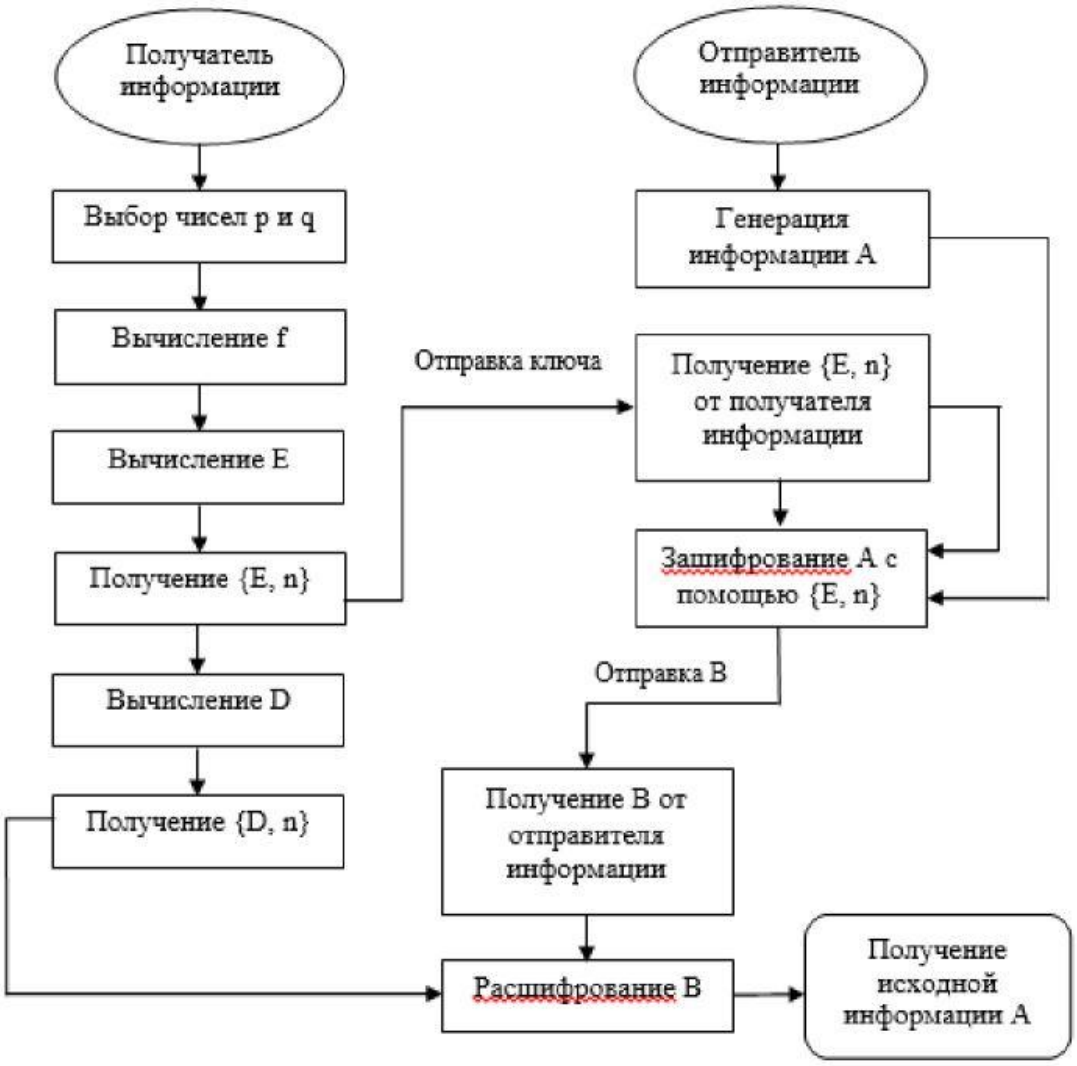

Рис. 1 Обобщенная схема работы алгоритма RSA

С началом цифровой эпохи появилась острая необходимость в защите информации в электронном виде от несанкционированного доступа и внесения изменений. Вопрос придания юридического статуса электронным документам долгое время оставался открытым, пока наконец не был разработан надежный способ их защиты - электронная цифровая подпись (ЭЦП, ЭП), которая считается аналогом рукописной и гарантирует защиту подписанного ею документа от малейших изменений.

В России начали применять ЭЦП в 1994 г., когда Главным управлением безопасности связи ФАПСИ при Президенте Российской Федерации был разработан первый отечественный стандарт такой подписи -

ГОСТ Р 34.10-94 "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма"

Электронные подписи разделяются Законом на три вида: простая, усиленная неквалифицированная (НЭП) и усиленная квалифицированная (КЭП) (ст. 5 Закона N 63-ФЗ). При использовании НЭП сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам НЭП может быть обеспечено без использования сертификата ключа проверки электронной подписи (ст. 5 Закона N 63-ФЗ). Усиленная КЭП обладает аналогичными возможностями и приобретается в аккредитованном удостоверяющем центре. Ее владелец получает открытый и закрытый ключи проверки ЭП и квалифицированный сертификат проверки ЭП.

Для создания ЭЦП в данный момент используют две программы: КриптоПро CSP или VipNet CSP. Все они работают на основании методов, рассмотренных выше. Рассмотрим процесс формирования и проверки электронной цифровой подписи.

Общепризнанная схема (модель) цифровой подписи охватывает три процесса:

- генерация ключей (подписи и проверки);
- формирование подписи;
- проверка подписи.

Механизм цифровой подписи определяется посредством реализации двух основных процессов:

- формирование подписи;
- проверка подписи.

Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения:

- осуществить контроль целостности передаваемого подписанного сообщения,

- доказательно подтвердить авторство лица, подписавшего сообщение,

- защитить сообщение от возможной подделки.

Схематическое представление подписанного сообщения показано на рисунке 2.

Рис. 2 Схема подписанного сообщения

Поле "текст", показанное на данном рисунке и дополняющее поле "цифровая подпись", может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в настоящем стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем, а также хэш-функции.

Рассмотрим работу программы КриптоПро. Введенный приказом Росстандарта от 7 августа 2012 года алгоритм формирования и проверки электронной подписи ГОСТ 34.10-2012, как и его предшественник ГОСТ Р 34.10-2001, базируется на операциях в группе точек эллиптической кривой. Однако новый стандарт поддерживает две длины ключей подписи, 256 и 512 бит, а при увеличении длины ключей вопросы выбора эффективных алгоритмов для промежуточных преобразований начинают иметь принципиальное значение для быстродействия. С учетом вида самих математических преобразований, трудоемкости конечных алгоритмов растут с увеличением длины ключа

быстрее, чем квадратичным образом, а значит, любые недостатки при выборе промежуточных алгоритмов неминуемо приведут к существенному падению производительности при большой длине ключа.

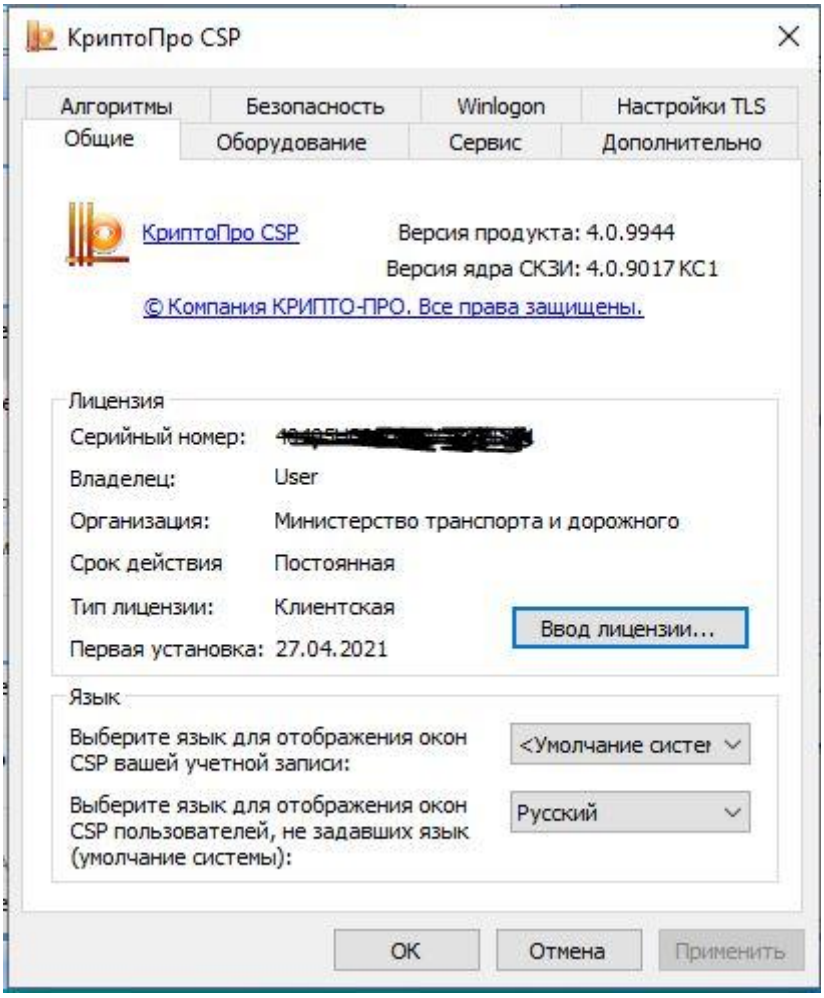

Рис. 3 Главное меню КриптоПро CSP

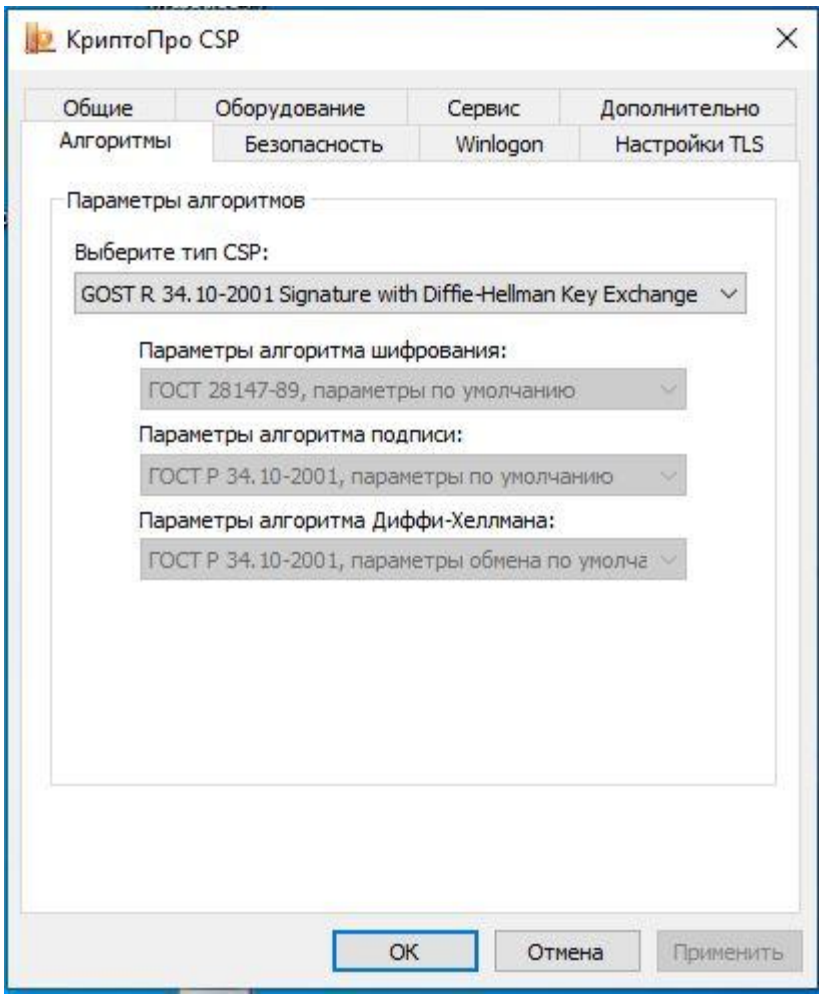

Рисунок 4. Алгоритмы работы программы

Одним из новых структурных решений в криптографическом ядре провайдера является выбор конкретных вычислительных алгоритмов в группе точек эллиптической кривой исходя из области использования той или иной точки (открытый ключ, промежуточная точка при вычислениях или порождающий элемент группы точек эллиптической кривой). Это позволяет существенно улучшить среднюю трудоемкость: на основе оценки целесообразности проведения предварительных вычислений, которые в дальнейшем используются для существенного ускорения всех последующих операций с той же точкой. В этих целях в коде реализованы три новых класса алгоритмов вычисления кратной точки эллиптической кривой (умножения точки кривой на скаляр).

Значения производительности реализаций алгоритмов в КриптоПро CSP 4.0 достигают следующих величин (данные получены на системе с Intel Core i5 3.3 GHz, Windows 7 x64, при работе в один поток):

1) скорость шифрования по ГОСТ 28147-89 в режиме гаммирования составляет 370 МБ/с;
2) скорость хэширования по ГОСТ Р 34.11-2012 (независимо от длины выхода) – 106 МБ/с;
3) 15756 и 3433 формирований подписей в секунду на коротких и на длинных ключах соответственно;
4) 9732 и 1853 проверок подписи в секунду на коротких и на длинных ключах соответственно.

Любое выдающееся достижение сопровождается значительными сложностями. Квантовые вычисления обсуждались в течение последних десятилетий, в то время как только ограниченное число компаний создали квантовые вычисления на ранних стадиях, ни одна из существующих операционных систем не может работать с квантовыми вычислениями. Компьютер нельзя разместить в помещении, как классические компьютеры, так как для его работы требуется система охлаждения, и он генерирует шум и тепло. В разделе "Квантовые вычисления: The Risk to Existing Encryption Methods" Кирш обсуждает экологические факторы риска и другие риски, такие как точность и фазовая ошибка. В исследовательской работе говорится: "Более высокая точность может быть достигнута при многочисленных испытаниях одной и той же задачи, но это уменьшает преимущество квантовых вычислений в скорости". Такой недостаток скорости замедлит время, необходимое квантовому компьютеру для взлома современных шифров. Даже если проблема точности решена, существует значительный риск для существующих шифров: классические компьютеры не способны противостоять атаке квантовых компьютеров.

Еще одна серьезная сложность, возникающая при внедрении квантовых компьютеров, связана с классическими алгоритмами шифрования. Классическому компьютеру для взлома конкретного алгоритма шифрования потребуются минуты, дни или даже годы, в то время как квантовый компьютер может выполнить ту же работу быстрее, чем классические компьютеры. "Однако квантовые компьютеры могут подходить к одной и той же задаче и пытаться найти несколько комбинаций одновременно, значительно сокращая время на поиск правильной комбинации". Поскольку квантовые компьютеры могут пробовать несколько комбинаций одновременно, на взлом пароля уйдет в разы меньше времени. Прежде чем внедрять квантовые компьютеры, математикам и компьютерщикам необходимо разработать более надежные алгоритмы, которые могли бы занять у квантового компьютера столько же времени, сколько потребовалось бы классическому компьютеру для расшифровки текста.

Классический компьютер использует биты для обработки информации, в то время как квантовый использует кубиты для обработки информации. Квантовые вычисления и угроза классическим методам шифрования" приводит слова другого автора: "Классические компьютеры обрабатывают информацию в битах, которые имеют два состояния: включенное (1) или выключенное (0); состояние бита не может быть одновременно включенным и выключенным". Однако квантовые компьютеры могут быть включены и выключены одновременно. "Квантовые компьютеры используют квантовые биты, также известные как кубиты, для обработки данных. Эти кубиты используют метод, известный как суперпозиция. При суперпозиции кубиты могут находиться в нескольких состояниях (включенном и выключенном) одновременно. Суперпозиция увеличивает возможности квантовых компьютеров по решению проблем". Квантовые биты позволяют компьютеру обрабатывать информацию быстрее, чем классический компьютер, поскольку он способен выполнять несколько действий одновременно. Это означает, что когда квантовые

вычисления станут общедоступными в ближайшем будущем, они будут обладать способностью атаковать системы с большей скоростью.

Вывод

Проведенный анализ показывает, что в современных системах криптографической защиты информации есть недочёты, как в квантовом мире, так и в обычном, не смотря на то, что технология является достаточно прочной к атакам. Разные криптопровайдеры показали приблизительно одинаковую скорость хеширования в одинаковых алгоритмах, разницу можно записать как погрешность. С развитием вычислительной мощности можно будет и усложнить процесс хеширования. Процесс шифрования данных на обычных компьютерах происходит достаточно быстро. Этой скорости с избытком хватает для подписывания обычных документов, не занимающих большие объемы данных. Что касаемо квантовых вычислений, они радикально меняют нынешние технологии, однако существуют определенные проблемы, которые необходимо решить. Важно найти альтернативы классическим методам шифрования, которые не будут работать при квантовых вычислениях. Крупные корпорации должны будут разработать стратегии защиты своих данных и, возможно, внедрить инфраструктуру квантовых вычислений. Криптовалютное пространство и технология блокчейн будут затронуты тем, что упростится проведение транзакций по цепочке блоков, а также ускорится добыча криптовалют. Изменится и электронная коммерция, создав более безопасное пространство для проведения онлайн-транзакций. Это может изменить все технологическое пространство, и все старые системы будут подвержены эксплойтам и должны будут идти в ногу с новыми технологиями, чтобы защитить себя от атак.

В будущем необходимо создать среду для квантовых вычислений с умеренными температурами. Чрезвычайно низкие температуры, которые требуются для квантовых вычислений в настоящее время, отпугивают больше

организаций. Все великое имеет свои плюсы и минусы, но в случае с новой технологией потребуется некоторое время, чтобы общественность приняла ее, но хорошо подготовиться ко всем проблемам, которые могут возникнуть с квантовыми вычислениями. Будет очень интересно увидеть, как квантовые вычисления станут более нормализованными, и посмотреть, как страны будут реагировать и обновлять эту новую технологию.