Глава 1.

1.1 Предпосылки становления гомоморфного шифрования

Постараемся рассмотреть предпосылки становления такого современного научного направления, как гомоморфное шифроване. Прежде чем мы перейдем к рассмотрению соответствующей научной области, мы рассмотрим основные этапы развития теории информационной безопасности вообще. Обладая относительно недавней историей, гомоморфное шифрование является закономерным развитием как методов анализа, так и фундаментальной теории криптографии.

Несмотря на то, что на сегодняшний день гомоморфное шифрование не поддается какой-либо строгой категоризации, для понимания процессов, которые вовлечены в это научное направление, важно предложить глубокий общий подход, который связан с динамикой развития фундаментальных исследований в других областях. Согласно этому подходу, можно условно выделить временные периоды в теории криптографии и шифрования вообще, которые охватывают различные смежные дисциплины, как, например, теорию чисел или теорию вычислительной сложности.

Постараемся выделить три таких периода, которые охватывают, условно говоря, различные временные масштабы, поэтому к ним больше применимо понятие „эры“.

1.1.1 Эра симметричного шифрования

Во-первых, выделим эру симметричного шифрования, которая обусловила возможность существования гомоморфного шифрования в таком виде, в котором мы его видим сегодня. Она длилась приблизительно до 1970-х годов прошлого столетия, создав такие специфические понятия понятия, как блочный и потоковый шифр, ключ, открытый текст и т. д. [1]. Можно сказать, что эта эра изучает способы конфиденциального хранения информации. Секретный ключ, который позволяет сохранить конфиденциальность зашифрованной информации даже при компрометации всей системы шифрования, стал фундаментальным понятием в криптографии и оказал наибольшее влияние на все последующее ее развитие [2].

При этом сформировались также и определенные методы как шифрования так и анализа зашифрованного текста. Можно выделить такие классические методы шифрования, как замена, перестановка, гаммирование. Сам по себе теоретический аппарат в теории характеризуется медленным развитием, однако, в военные и послевоенные годы они получают мощный толчок, которому способствовали внешние условия: развитие радиосвязи, появление теории информации (Шеннон) и теории алгоритмов (Тьюринг). Теория информации обусловила появление способов изучения информационных свойств сообщений путем количественного анализа (так мы можем говорить, например, о переборе методом грубой силы), а теория алгоритмов обусловила практическое применение криптографии на вычислительных устройствах вместо механических, а также развитие теории вычислительной трудоемкости.

Примером теоретических достижений в современной теории симметричного шифрования является появление концепции одноразового блокнота, появление таких алгоритмов для преобразования открытого текста в шифртекст, которые описываются не одиночными математическими операциями, а сложными логическими примитивами, такими как, например, ячейки Фестеля, как следствие, появилась стандартизация криптографических примитивов, и в дальнейшем блочных и потоковых шифров. Ярким образцом стандартизации является блочный шифр DES [3], представляющий собой набор документов и рекомендаций, утвержденных на государственном уровне и используемых в экспортной политике. [4].

Актуальным и одновременно отдельным направлением симметричного шифрования являются генераторы ПСП [Полуяненко-17], образующие криптографическую стойкость детерменированных устройств, операционных систем и многих криптографических пакетов, таких, как OpenSSL. Для генераторов ПСП (или генераторов потокового шифрования) наболее развитой областью является теория регистров сдвига с линейной обратной связью. Примерами являются генераторы Yarrow и LRNG. [5][6]

Также можно выделить такое современное актуальное направление в симметричном, как аугментация существующих громоздких криптографических систем под нужны устройств с низкой вычислительной способностью, как, например, для интернета вещей. Это направление носит название легковесной криптографии, «Lightweight Cryptography». [7]

1.1.2 Эра асимметричного шифрования

С 1970 годов можно обозначить начало эры ассиметричного шифрования, которая характеризуется фундаментально работой по RSA [8], реализовавшей обмен ключами Диффи-Хеллмана. Ассиметричные системы подняли новые вопросы не только для конфиденциального хранения информации, но также и для ее передачи, или, иначе говоря, они обусловили активное использование такого элемента, как канал связи в системах шифрования. Начинают формироваться методы анализа на основе комплексности/сложности проблем (NP-проблемы, P-проблемы и NP-полные), а также появляется понятие криптографических примитивов, например, односторонние функции. [2]

Во второй эре можно выделить несколько этапов, длящихся, условно говоря, по одному десятилетию.

Первый этап эры асимметричного шифрования

Первый этап 1970-1980 гг. предлагает фундаментальные исследования и поиск новых математических примитивов благодаря работе [2], которая обозначила новое направление развития или другой угол зрения на тот момент в теории криптографии.

Все это касается именно фундаментальной криптографии, здесь начинают формироваться сами категории криптографических примитивов и протоколов. Вводится понятие односторонней функции [2]. Появляется многообразие протоколов, среди которых можно выделить разделение секрета [9] и электронную подпись [10].

Особое внимание получает теория чисел, благодаря которой [2] создаются предпосылки для изучения новых математических примитивов, например, конечных полей [11], и вывислительных проблем, например, факторизации [8].

Как уже говорилось выше, развитие получает теория вычислительной сложности [12], вместе с которой появились другие модели атак по открытому тексту, шифртексту и выбранному шифртексту.Важной является теорема Брассарда о приведении к NP-полной задаче [13].

Важно отметить также первую работу по гомоморфному шифрованию [14], в которой оно определеляется под «приватным гомоморфизмом». Здесь эта область криптографии находится в состоянии зарождения, и более-менее интенсивное развитие гомоморфное шифрование получит лишь спустя несколько десятилетий.

Второй этап эры асимметричного шифрования

Второй этап 1980-1990 гг. характеризуется дальнейшим развитием общей теории, но уже больше поисковыми и прикладными исследованиями, особенно в части новых криптографических протоколов. Все направления, зародившиеся на прошлом этапе также получают свое дальнейшее развитие.

Изыскиваются новые вычислительные проблемы, которые обуславливают появление различных классов криптографических систем. Появляются вероятностные системы шифрования и вероятностный анализ. Имевшая ранее более целостную структуру криптография подвергается пересмотру и более глубокому анализу, предлагая потенциальную возможность синтеза систем шифрования. Появляется понятие системы шифрования вообще, понятие системы с открытым ключом. Теория чисел и область, где она используется (простые числа, сравнения и модульная арифметика), даёт возможность строить такие системы на следующих вычислительных проблемах: факторизация, дискретный логарифм, квадратичный логарифм [15], возведение в степень [8]. Появляется криптография на эллиптических кривых [16].

Как уже было написано, продолжают исследоваться новые криптографические протоколы. Это направление проявляет себя, как наиболее активный процесс в исследованиях [17, с.315/4]. В результате появляются такие протоколы, как, например, протокол электронной подписи [10], протокол забывчивой передачи [18], протокол сертифицированной почты [19], протоколы выборов [20] [21] и др.

Некоторые «фокусы» (невоспринимавшиеся всерьез умственные модели/абстакции) [17], например, с подбрасыванием монеты, начинают рассмативаться, как серьезная теория, которая становится основой в некоторых пртоколах, таких как, например, протоколы выборов и подбрасывания моне-

ты [22] [23]. В дальнейшем это приводит к открытию теории доказательств с нулевым разглашением, сыгравшим большую роль в будущем контексте вычислительной криптографии [24] [25]. Отметим также еще один шаг в направлении гомоморфного шифрования; он происходит совместно с работой по развитию приватного гомоморфизма [26].

Наиболее важным событием, оказавшим большое влияние на фундаментальную теорию, можно исследование вероятностных систем шифрования [27]. Это позволило рассматривать криптосистемы с позиций набора новых свойств, например, семантической защищённости, и новых примитивов: односторонних предикатов и функций с потайным входом. Это означает, что для потенциальной возможности синтеза криптосистем и, отдельно, систем шифрования, которая была описана выше, добавляются новые строительные блоки; появляется многообразие параметров, которые можно задавать и варьировать в процессе разработки системы.

В дальнейшем асимметричное шифрование находим множество практических применений, особенно, с развитием сети интернет.

Третий этап эры асимметричного шифрования

Третий этап 1990-2000 гг. – это этап усложнения и интеграции. В этом периоде исследователи обращают свой взор на выявление взаимосвязи в структуре теории вообще. Окончательно формируется теория анализа на основе комплексности. Кроме этого, исследователи обращают свое внимание на квантовую архитектуру, изучая методы анализа, применимые на ее основе. [28]

Интеграцию различных классов криптосистем друг в друга, а также их усложнение можно проследить, например, в разработке вероятностных доказательств с нулевым разглашением [29]. Многие протоколы становятся многосторонними (multiparty computations) [30], и также формируется анализ, который принимает во внимание несколько сторон и возможности участников, например, атака Сивиллы. Здесь можно выделить «статические» (или классические) протоколы, например, протоколы торгов, выборов, совместной подписи и расшифрования или threshold-протоколы. Это протоколы, которые предлагает асимметричная криптография. Наряду с ним появляются «динамичные»

(гомоморфные) протоколы, не имеющие прямое отношение к приватному гомоморфизму, но, тем не менее, развивающие его. Это протоколы анонимных запросов пользователей к базам данных (защищенные индексы) и совместные вычисления (запросы) баз данных между собой [31]. Развитие же самого приватного гомоморфизма можно обнаружить по косвенному влиянию. Авторы различных криптосистем сами пытаются исследовать свои системы на гомоморфные свойства. Все эти процессы происходят в рамках одной работы. Так, например, обнаруживается много систем с частичным гомоморфизмом [32] [33]. Появляются также примитивы, относящиеся непосредственно к вычислительной криптографии: позволяющие выделять определенные вычислительные механизмы из других систем NC-цепи [34] и перешифрока шифртектса «на ходу» (Atomic Proxy Cryptography) [35].

Усложнение прослеживается и в многообразии новых свойств, которые можно обнаружить теперь применительно к криптографической схеме, а не для шифртекста или его параметров. Такими свойствами являются, например, негибкость [36] [37], семантическая защищенность [38], «самоослепление» [33], неразличимость, доверие, корректность, приватность, аутентификация, идентификация, анонимность, отслеживание, treshhold и т. д. Эти свойства получили определение, как придающие твердость [Robustness; wiki] криптографической схеме. Как следствие для свойств твердости, обнаруживаются и новые методы анализа, виды атак, например, приведение к другой (чаще полиноминальной) проблеме, компьютерная симуляция, случайная саморедукция [39], случайный мэппинг. [17, с.317/2]

За счет оказанного киптографией влияния окончательно формируется теоия комплексности, которая обнаруживает избыточность комбинаторных (ранцевых, knapsack) проблем [40]. С помощью теоремы Брассарда была сформулирована важная теорема о том, что детерменированная система или система с оператором эквивалентности обладает полиноминальной стойкостью и вскрывается за линейное время в отношении длины ключа [41].

К вниманию исследователей предстают новые вычислительные задачи, связанные с решетками и их применением [WorstAverage-97] [42] [43]. В итоге появляется криптография, которая основана решетках структур идеалов, например, колец, NTRU [44]. Работы предыдущих лет анализируются на предмет структуры и наличия проблемы решеток, к которым они при возможности, соответственно, сводятся. Кроме решеток, для всех остальных вычислительных

задач, остаются изыскиваться только системы, построенные на проблемах факторизации (и другим проблемам теории чисел, которые связаны с конечным полем и понятием простого числа, например, задача о сумме подмножеств), линейным кодам и эллиптическим кривым.

На примере AES можно выделить становление синтеза криптографических систем [4]. Несмотря на то, что в конкурсе участвовали кандидаты для блочных шифров, условия конкурса показывают, как можно задавать параметры для криптосистемы вообще. Можно также выделить направленность синтеза применительно именно к системам шифрования - грубо говоря, существует некоторый уровень абстракции, позволяющий строить системы шифрования различных классов по общим принципам.

До сегодняшнего дня асимметричная криптография воспринимается, как наиболее используемое, комплексное и практичное направление, имеющее наиболее интенсивное развитие. Прослеживается тенденция развития и трансформации протоколов взаимодействия для двух сторон в многосторонние протоколы. Само понятие криптосистемы прочно связалось с понятием асимметричной системы шифрования.

Важно отметить, что асимметричная криптография не может отойти от концепции центральной базы данных, узлового источника, обладающего доверием. Именно на этой идее получает внимание вычислительная криптография, представленная следующей эрой.

1.1.3 Эра гомоморфного шифрования

С 2000 гг. по настоящее время развивается эра гомоморфного шифрования. Ее можно охарактеризовать еще большими усложнениями, комплексностью, междисциплинарным взаимодействием, развитием технологии WWW. Вопросы криптографии, лежавшие на поверхности, теперь требуют более глубокого анализа, что повышает требования к квалификации исследователей. Формируется междисциплинарная связь между криптографией и другими научными областями, например, теорией множеств, теорией игр, теорией телекоммуникаций. [45] Все это способствует условиям для обнаружения полностью

гомоморфной системы шифрования. Эту также можно разделить на несколько периодов.

Первый этап эры гомоморфного шифрования

Первый этап 2000-2010 гг. является этапом междисциплинарной интеграции. Начинают захватываться области различных компьютерных наук, как, распределенных вычисления, архитектура и пр. Так, например, появляются аппаратные криптографические акселераторы. [Advances Crypto-07]. Появляется возможность стандартизации криптографических протоколов (IPSec и SSL).

Усложнение и междисциплинарность можно продемонстрировать, например, в случае мультисторонних протоколов, которые приобретают элементы теории игр [46] [47]. В 2000-х годах теория множеств оказывает влияние на криптографию, где ведется поиск новых математических структур, например, полукольца [48] и якобианы [49].

Получает развитие теория решеток, а именно поблема худшего/среднего [50] [51] [52] [53]. Как следствие, получает внимание и NTRU [54][55]. В качестве новых вычислительных проблем, кроме решеток, можно выделить шифрование на основе 2-NDF формул [56].

Установился набор проблем, которые можно признать классическими в теории криптографии: для симметричного шифрования - логарифм, факторизация, возведение в степень [57] [58], и, отдельно, ранцевая укладка [59] [60]; для ассиметричной криптографии - модульная арифметика Диффи-Хеллмана, факторизация и логарифирования для систем RSA и Эль-Гамаля, цифровые подписи Шамира и, отдельно, ранцевая укладка Меркле [61]. Для этих проблем, соответственно, появляются более глубокие методы анализа, например, адаптация алгоритма Полига-Хеллмана для редукции задачи дискретного логарифмирования [48].

На фоне всего этого развиваются опасения, подкрепляемые теорией квантовых вычислений [62].

В конце-концов, исследователи постепенно приходят к системах неполного гомоморфного шифрования [63] [64] [TOpMult-08] [65]. Развитие фундаментальных направлений, осознание взаимосвязей элементов криптографических

систем позволило создать предпосылки для синтеза первой гомоморфной системы шифрования. Отдельно от этого развивается такое экзотическое направление, как вычисление ветвлений [66], которое можно поставить в один ряд с NC-цепями. Несмотря на то, что подобные работы лишь косвенно относятся к гомоморфному шифрованию, их все же можно приписать к более общей вычислительной криптографии. Но, тем не менее, совокупность „косвенных“ работ внесет равнозначный вклад совместно с теорией решеток для работы Джентри [67], которая исследует первую полностью гомоморфную систему шифрования в следующем этапе. [68]. К вычислительной криптографии относится и появление такой концепции, как обфускация данных. Это также говорит о стремлении исследователей обеспечить приватность, но уже не данных, а самого кода или алгоритма для программы обработки. [69] [70]

Второй этап эры гомоморфного шифрования

Наконец, 2010-2018 год – этап гомоморфного шифрования, облачных вычислений и, одновременно, период пост-квантовой криптографии; все направления можно признать равнозначными. Именно в последнее десятилетие системы гомоморфного шифрования получили наибольшее развитие [AsurveyOnHomoEnc-16]. Вызвано это вниманием общества к, так называемым, облачным вычислениям. В виду некоторого появившегося разнообразия гомоморфных систем стала возможна их классификация.

Выдвинутые в 1970-х годах Диффи и Хеллманом предположения о том, что NP-задачи устойчивы к атакам компьютерных алгоритмов, оказались неспособны противостоять системам на квантовой архитектуре. Представленный Шором 1994 году алгоритм позволяет с помощью свойства запоминания информации в кубитах эффективно распараллеливать NP-задачи. Кроме этого, прогресс в разработке квантовых компьютеров оказался достаточно быстрым, так что средняя организация уже к 2030 году сможет купить квантовый компьютер за 1kk долларов. Поэтому исследователи начинают обращать внимание на угрозы, исходящие от квантовых компьютеров. Алгоритмы, поддерживаемые NIST признаются слабыми; в них входят RSA, DSA и EC. Для оставшихся

алгоритмов (AES) рекомендуемая длина ключа увеличивается с 80 бит до 112 и 128 бит. [NIST IR 8105]

Ведутся поиски новых примитивов, обладающих криптографической стойкостью для анализа алгоритмом Шора. В числе таких примитивов оказываются линейные коды, решетки и полиномы с множеством переменных (мультивариативные полиномы).

Исследования Джентри, которое показало принципиальную возможность существования полностью гомоморфного шифрования, соответствующее направление «облачных вычислений» начинает занимать огромное влияние. Появляются улучшения для системы Джентри, исследуются новые полностью гомоморфные системы; также происходит процесс преобразования некоторых полностью гомоморфных системы в частично- и полностью гомомофрные системы с целью повышения производительно и более практических реализаций за счет ослабления гомоморфной структуры. Остаются открытыми некоторые вопросы безопасности гомоморфных систем, например, KDM, семантическая защищённость, устойчивость к атакам по выбранному шифртексту (устойчивость к атакам по подобранному шифртексту невозможна в-принципе, так как гомоморфный текст не негибкий). [ASurveyOnHomoEnc-16]

В качестве новых направлений для исследования в гомоморфном шифровании можно определить функциональное шифрование – это шифрование для выбранных атрибутов или для определенных пользователей, так называемые системы шифрования с порогом (Threshold Full Homomorfic Encryption).

Гомоморфное шифрование занимает свое место в теории криптографии, где криптография как бы пытается стать непрерывной, уйти от дискретных элементов.

На данный момент разработаны эффективные алгоритмы полностью гомоморфного шифрования.

1.2 Теория гомоморфного шифрования

Работа Джентри позволила открыть существование полностью гомоморфных систем. Его результат - не просто конкретная схема, а набор инструментов и методик для получения таких схем, например, на основе огра-

ниченно-гомоморфных систем. В-частности, это же может быть применимо и к гомоморфному шифрованию, как к основному элементу таких систем. Чтобы шифрование можно было назвать гомоморфным, оно должно позволять выполнение неограниченного числа операций над шифртекстом. Это подразумевает также, что должно выполняться следующее свойство - размер шифртекста должен оставаться в заданных пределах./par После схемы Джентри интерес к гомоморфному шифрованию значительно возрос во всем мире, наиболее значимые результаты были достигнуты в течении последних 10 лет.

Первой работой по гомоморфному шифрованию принято считать [RivestDataBanks-78]. Развитие описанные идеи получили в работе Брикеля и Якоби “On privacy homomorphisms”. В течении последующих 30 лет удавалось получить лишь частичные результаты, то есть такие системы, где поддерживалось бы гомоморфное либо сложение, либо умножение, но ни обе операции вместе. Такие системы носят название, соответственно, частично гомоморфных систем (PHE). [AsurveyOnEncSchemes].

В 1980-х со становлением вероятностной криптографии формируются требования к гомоморфным системам: способность выполнять любые операции (под любыми обычно понимаются умножение и сложение) в неограниченном количестве, обладать семантической защищенностью. Также должно выполнятся требование на ограниченное увеличение размера шифртекста после каждой операции, что косвенно отражает свойство отсутствия ограничений на количество выполнений.

Далее, в 1990-х теория алгоритмов позволила создать удобные представления для вычислений. Модель вычислений теперь может задаваться не только формулой, но и графом, таблицей истинности, булевой функцией, логической цепью, конечным автоматом и т. д. С 2000-х годов начинают развиваться почти гомоморфные системы (Somewhat Homomorfic Encryption) – это такие системы, которые могут выполнять как операции сложения, так и операции умножения, но в ограниченном количестве.

Затем, начинают затрагиваться все уровни криптографической структуры, приводящее, таким образом, к тому, что Джентри синтезирует полностью гомоморфную систему, развитие которой вылилось в три поколения. В процессе развития этой системы, появилась возможность изучить особые свойства гомоморфных систем, появилась более глубокая теоретическая база. Кроме этого, появилось направление, которая уделяет особое внимание функциям вычисле-

ний – обфускация. На данный момент гомоморфные криптосистемы имеют эффективные алгоритмы, а вектор их равития лежит в направлении интегрирования и дальнейшего усложнения.

За все время была выработана следующая классификация для гомоморфного шифрования: частично-гомоморфное, ограниченно-гомоморфное и полностью гомоморфное шифрование.

1.2.1 Частичное гомоморфное шифрование

Список частично-гомоморфных систем представлен ниже:

#	Год	Название	Операции		Вычислительная проблема	Улучшение какой системы	Примитив, свойства
	Частично гомоморфные системы						
1	1978	Система RSA		*	Факторизация [Montgomery-94]		
2	1982	Система Гольдвассер-Микали	?		Проблема квадратичных вычетоа (Quadratic Residuosity Problem) [Kalinski-2005]		Вероятностная криптосистема, зашифровывает побитно
3	1985	Система Эль-Гамаля		*	Дискретное логарифмирование [Kevin-90]	Система RSA	
4	1994	Система Бенало	+		Вычеты произвольной степени (Higher Residuosity Problem) [BenalohRooting-87]	Система Гольдвассер-Микали	Вероятностная криптосистема, зашифровывает блок данных в виде полинома
	1998	Система Накаша-Штерна	+		Вычеты произвольной степени (Higher Residuosity Problem)	Система Бенало	Улучшение производительности за счет изменения схемы расшифрования
	1998	Система Окамото-Утиямы	+		Квадратичные вычеты, факторизация	Система RSA, система Гольдвассер-Микали	Вероятностная криптосистема, улучшение производительности за счет использования других множеств

5	1999	Система Пэйе	+	K	Комплексные вычеты (Composite Residuosity Problem) [Jager-12]		Можно добавить гомоморфное умножение, если знаешь открытый текст одного из сообщений, умножение на скаляр, вероятностная криптосистема
	2001	Система Дамгода-Джурика	+			Система Пэйе	Вероятностная криптосистема
	2002	Система Гэлбрейта	+			Система Пэйе	Эллиптические кривые
	2007	Система Кавачи	+		Поиск решения на решетках		Большая циклическая группа, решетки, псевдогомоморфизм

Можно выделить следующие вычислительные проблемы, на которых может быть построен частичный гомоморфизм:

1. Факторизация
2. Квадратичные вычеты, вычеты произвольной степени
3. Композитные вычеты
4. Решетки
5. Дискретное логарифмирования
6. Линейные коды

1.2.2 Ограниченно-гомоморфное шифрование

Отдельные механизмы были выработаны в классе ограниченно-гомоморфных систем. Особенностью этого класса является возможность конструирования функции, элементарные же функции состоят из базиса булевой алгебры.

Для этого класса характерно использование бинарных таблиц и забывчивой передачи, как основных элементов при построении системы. Проблемы, которые необходимо решить при этом - это ограничение на рост размера шифртекста, а также реализация устойчивого протокола с фиксированным количеством раундов. В первой такой системе, которая припысывается Яо [Yao-82], участники общаются каждый раунд и узнают, нужна ли помощь в формировании выходного значения до тех пор, пока не будет пройдена вся цепочка вычислений. В этом случае глубина вычислений – основной фактор, который влияет на комплексность криптосистемы.

Система Сендера [Sender-99] является развитием системы Яо; в его системе в качестве входного значения используется полином, вычисляющийся с использованием NC-цепей, поэтому все операции происходят за один раунд. Однако, в этом случае размер шифртекста растет экспоненциально, так как основной ограничивающий фактор не глубина вычислений, а рамер бинарной таблицы.

Качественный скачок в развитии представляет система Бонеха-Го-Ниссима [Boneh-05], которая вычисляя 2-DNF-формулы над шифртекстом, обеспечивает как алгебраический набор операций, так и константный размер шифртекста.

Система Ишая-Пашкина расширяет область гомоморфных вычислений на ациклические графы принятия решений, более генерализированным множеством, чем таблица истинности.

Особенностью вышеперечисленных систем является использование бинарных операций вместо алгебраических, что не позволяет им полностью соответствовать классу алгебраически гомоморфных систем. Таким системы, также, являются особым случаем для теоремы Бонех и Липтона, которые показали, что детерминированные алгебраически гомоморфные системы над кольцами Z/NZ могут быть сломаны за время не выражающееся экспоненциальной зависимостью. Но для систем $Z/2Z$ необходимо выполнение условия вероятностной системы, если они реализуют гомоморфные вычисления.

#	Год	Название	Операции		Математический примитив	Криптографический примитив	Размер шифртекста
1	1982	Система Яо [Yao-82]	AND	OR	$Z/2Z$	Искаженная схема (garbled circuit), забывчивая передача (oblivious transfer)	Растет линейно с каждой элементарной операцией; переменное количество раундов в протоколе, которая зависит от глубины вычислений
2	1994	Система Феллоуза-Коблица, “Polly Cracker”	+	x			Размер шифртекста растет экспоненциально после каждой операции
3	1999	Система Сендера [Sender-99]	AND	1-OR или 1-NOT	$Z/2Z\,[x]$	NC^1-цепи, забывчивая передача	Шифртекст растет экспоненциально, гомоморфизм на основе полугруппы, один раунд в протоколе

4	2005	Система Бонеха-Гоу-Ниссима	+	1-х	$Z/2Z\,[x]$	2-DNF формулы	Проблема подмножеств [Gjosteen-04], шифртекст имеет константный размер
5	2007	Система Ишая-Пашкина	+			Ациклический граф (вычисление ветвлений, binary desicion diagrams)	Вероятностная криптосистема, не зависит от размера функции

Отдельного внимания заслуживает система Мельчора [Melchor-10], которая опубликовалась после работы Джентри и которая разработала способ цепного шифрования, где каждое звено для этого шифрования может быть сформировано на основе примитива из другой существующей криптосистемы. Цепное шифрование позволяет производить гомоморфные вычисления заданной глубины, которая зависит от количества используемых примитивов их свойств, от чего также зависит наличие набора алгебраических операций.

1.2.3 Полностью гомоморфное шифрованияе

Система Джентри в качестве своей основы использует решетки [67], которые также получили огромное внимание после его работы. Решетки признаются устойчивыми к квантовому анализу [71], кроме этого они имеют достаточно обширный теоретический фундамент, поэтому их использование можно отнести к достоинствам системы. Теория решеток впервые была опубликована в [Minkowski-68], с тех пор было разработано несколько достаточно стойких вычислительных задач, наиболее используемыми из которых являются задачи поиска ближайшего и кратчайшего вектора [72] и проблема среднего/худшего [73]. В [74] выл представлен способ вычислительной редукции решеток, что напрямую связало их с теорией криптографии. Решетки могут комбинироваться с другими математическими примитивами, что определяет различные классы таких систем.

Так, например, система Джентри относится к классу систем, построенных на решетках идеалов. Подобное решение позволило реализовать ассиметриченую гомоморфную систему шифрования, то есть систему с публичным ключом

[75]. Однако, она довольно сложна в реализации и имеет некоторые недостатки в плане производительности, особенно это касается перешифровки шифртекста. За последние годы было предложено много способов ее оптимизации. В 2010 году предложено улучшение схемы генерации ключа, а также улучшение стойкости гомоморфного шифрования [76]. Вариант схемы Джентри, работающий на шифртексте и ключе меньшего размера без потери стойкости был представлен в [77]. Поздние работы направлены на дальнешее улучшение алгоритма генерации ключа и также алгоритма "перешифровки"шифртекста. Также разработана ограничено-гомоморфная схема с пространством открытого текста большей мощности, что увеличивает количество гомоморфных операций [78]

Существует класс систем на решетках, которые используют проблему LWE [79] и ее алгебраический вариант - ring-LWE [80]. Эти проблемы признаются наиболее стойкими, так как они позволяют использовать меньший размер шифртекста без потери защищенности. В 2011 году была предложена схема ограниченного гомоморфного шифрования [81] на основе RLWE, где была показана большая производительность, чем в LWE. Эта схема в той же работе была дополнена до полностью гомоморфной схемы.

Все гомоморнфые схемы появившиеся после этой работы принадлежат к категории систем второго поколения, например, система использующая технику перелинеаризации [82], которая устанавливает стабильный размер для шифртекста большого размера и обходится без процедуры перешифровки шифртекста. В качестве тенденций развития можно обозначить уровневые системы полностью гомоморфного шифрования, которые повышают производительность за счет использования функций с ограниченной глубиной вычислений (ограниченным набором элементарных операций) [83], линейный рост ошибки с каждой операцией [72], а также системы с шифрованием атрибутов (идентификацией, множественными ключами) и собственными векторами [84]

Актуальной схемой для доработки полностью гомоморфногом шифрования является схема [85], которая использует проблему аппроксимации общего делителя, поддерживая большую мощность пространства сообщений.

Одним из самых перспективных направлений в гомоморфном шифрованиии является класс NTRU-систем, также использующих решетки. В 2009 году NTRU упоминается в работе Джентри [86, p.65], как первая криптосисте-

ма, использующая структуры идеалов на решетках. Первая работа по NTRU [75] была опубликована в 1988 году Хоффштейном, Пифером и Сильверманом и изначально подразумевала собой криптосистему с публичным ключом на кольцах, которая лишь в дальнейших работах получила развитие и связь с решетками (1997-2001 год) [May-99; 87; 88]. В дальнейшем NTRU-криптография строится вокруг работы Миклоша Айтая [89], на его принципе эквивалента среднего/худшего; цепочка работ, развивающих проблематику NTRU [90—94] вышла в период с 2002 по 2007 годы. Параллельно работы Хоффштейна [75; 95] представили алгоритмы шифрования и электронной подписи, криптографическая стойкость которых была исследована в работе [Stehl\IeC {\'e}-11].

Дальнейшее развитие NTRU получило с выходом серий работ, представляющих системы NTRU-LWE и NTRU Prime [96].

Несмотря на то, что с момента появления NTRU-шифров прошло более двух десятилетий, NTRU-схема получила внимания лишь после открытия полностью гомоморфного шифрования и возросшего интереса к криптографии на решетках. Оба вопроса являются перспективными для NTRU, что делает его актуальным направлением в современной криптографии, особенно, учитывая что NTRU обладает хорошей асимптотической производительностью и малым размером шифртекста. [97; 98]

Возможность существования полностью гомоморфного шифрования на NTRU было впервые показано в [99] и [100]. Помимо проблемы решеток, система [99] также строится на мало изученной проблеме Decisional Small Polynomial Ratio (DSPR). В [101] схема была избавлена от DSPR. Последовательно [102] показал технику тензорирования, с помощью которой можно ограничить рост ошибки при гомоморфных операциях и также избавиться от DSRP. Однако, это техника требует большого размера ключа вычислений и комплексность в протоколе при ключевом переключении, что делает схему непрактичной. Все схемы, которые пытаются уйти от DSRP уязвимы к определенному виду атак. В 2016 году [Doroz-16] появилась модицифированная схема FHE для NTRU, не использующая DSRP и, кроме этого, не требующая ключ вычислений при произведении гомоморфных операций, что делает схему очень привлекательной для исследователей. Вместо этого она использует технику выравнимания шума [103], которая была получена из схемы Джентри [104].

Актуальными направлениями для NTRU на данном этапе является дальнейшее получение практической FHE схемы, что является критически

необходимым шагом, а также реализация вычислительного потенциала за счет оптимальной аппаратной реализации [Doroz-14,Dai-14,LiuWu-15]. Перспективной является также предложенная в 2014 году схема [Rohloff-14], где используются элементы самонастройки [Alperin-13] и "double-CRT"[Gentry-12] для преобразования шифртекстов в соответствии с текущей задачей.

Одним из вариантов, не связанных с решетками, является схема, предложенная [VanDijk-10]. Эта схема использует ограниченно-гомоморфную схему, построенную на целых числах и модульной арифметике, которая затем использует метод Джентри для получения полностью гомоморфной схемы за счет "самонастройки"(bootstrapping).

Вычислительная сложность системы базируется на задаче аппроксимации поиска наибольшего общего делителя [Galbraith-16].

На данный момент реализована симметричная и ассиметричная гомоморфная система на целых числах; особенностью данной схемы является простота в реализации, взамен схема обладает низкой вычислительной способностью.

Основные направления развития данного класса систем включают уменьшение размера публичного ключа [Coron-11] [Coron-12] [Yang-12], а также улучшение алгоритмов генерации ключей [RamaiahKumari-12] и перешифровки [Chen-14]. Также существует версия с упаковкой шифртекстов [Cheon-13]

На данный момент существует множество подходов к улучшению системы на целых числах: масштбируемое инвариативное полностью гомомофное шифрование [Coron-14], схема с открытым текстом в виде целых чисел [RamaiahKumari-12], ограниченно-гомоморфная система с арифметикой больших чисел [Pisa-12], полностью гомоморфная схема без самонастройки [Aggarwal-14], а также схема в небинарном пространстве сообщений [NuidaKurosava-15].

1.3 Криптографическая структура

На основе анализа, произведенного выше, можно утверждать, что процесс развития криптографии последователен в направлении гомоморфного

шифрования. Если симметричная криптография рассматривает вопросы конфиденциального хранения информации, то асимметричная криптография рассматривает вопросы конфиденциальной передачи информации, или, говоря по-другому, криптографические протоколы. Вычислительная криптография рассматривает аспект конфиденциальных вычислений, причем это относится как к данным, над которыми производятся вычисления, так и к алгоритму, по которому они производятся. Сама же последовательность развития заключается в том, что симметричная криптография может быть интегрирована в асимметричную, а та в свою очередь может быть также интегрирована и рассмотрена с точки зрения вычислительной криптографии. Так, например, в криптографических системах асимметричный протокол исследуется для выработки и передачи секретных ключей, основной же канал передачи данных строится на основании симметичного шифра. В то же время как, и в симметричных, так и в ассиметричных системах могут быть обнаружены элементы гомоморфизма.

Соответственно, не каждая система может обладать гомоморфными свойствами, и не каждый примитив из симметричной криптографии может использоваться при построении ассиметричной системы. Описанные отношения представлены на рисунке ниже.

Рисунок 1.1 — Криптографическая структура

Также на рисунке обозначены отдельно две области: квантовая криптография и обфускация. Обфускация сама по себе не является частью вычислительной криптографии, однако является производной от нее. В качестве довольно актуального направления, обфускация представляет собой способы обеспечения кофиденциальности, но не пользовательских данных, а самих алгоритмов обработки.

Квантовая же криптография не затрагивает гомоморфное шифрование напрямую, но так как асимметричное или симметричное шифрование может быть частью системы с гомоморнфым шифрованием, то развитие этого направления может оказывать непосредственное влияние.

Чтобы показать динамику развития, можно отобразить условные элементы, которые представляют собой некоторый уровень абстракции над любой системой шифрования. Для этих элементов выделяются четыре уровня абстракции. Эти уровни затрагиваются в различной мере на различных этапах развития теории шифрования и криптографии, за счет чего и обладают качеством выражения динамических свойств. Этими уровнями являются: уровень вычислительной проблемы, уровень математических примитивов, уровень криптографических примитивов и уровень криптографической схемы.

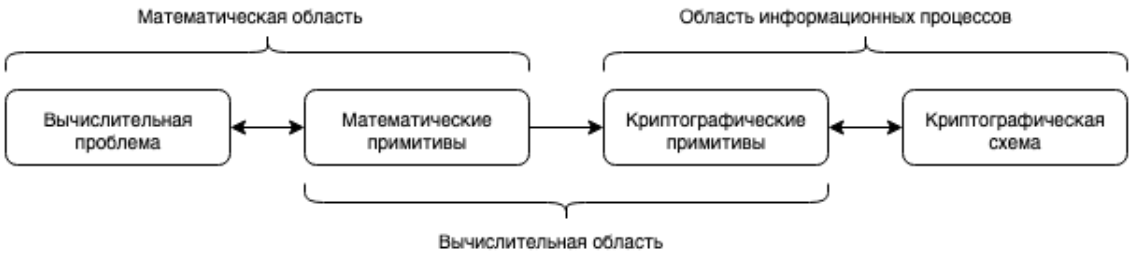

Рисунок 1.2 — элементы системы гомоморфного шифрования

Вычислительная проблема характеризует, насколько величина перебора входных данных по значению шифртекста близка по сравнению с граничным значением, представляющим экспоненциальную зависимость от длины шифртекста (значение 2 в степени длины шифртекста). Иными словами, она характеризует качество того, что входные данные нельзя подобрать за время, имеющее полиноминальную зависимость от длины шифртекста.

Набор математических примитивов задаёт множество значений (символов) для шифртекста, его структуру, а также определяет элементарные операции над ним, которые образуют уровень вычислительной проблемы - параметр, связывающий преобразования из открытого текста в шифртекст.

То, какую задачу организует вычислительная проблема посредством математических примтивов, а также функциональное назначение криптосистемы в целом задают криптографические примитивы, например, односторонние функции. Криптографический примитив в системе шифрования определяет, как вычислительная проблема может быть редуцирована, то есть обеспечивает существование неких секретов или ключей.

Наконец, криптографическая схема реализует непосредственно понятие ключа и протокола, то есть модель для конечного использования всей криптосистемы (системы шифрования).

Можно увидеть, что на заре развития теории криптографии, основополагающими уровнем был уровень криптографического примитива, на основе которого изыскивались различные методы шифрования. До асимметричной криптографии никто не мог предположить наличие элементов для криптографической схемы, поэтому можно сказать, что уровни криптографических примитивов и криптографической схемы совпадают, то есть для эры симметричного шифрования не было четкого разделения на уровне вообще, как и понятия системы шифрования.

С появлением асимметричной криптографии появилось наличие публичного/секретного ключа, которым описывается работа криптографической схемы.Для этой эры характерно четкое осознание всех уровней, но основные направления исследований сосредоточены на области информационных процессов и протоколов, в которую входят криптографические примитивы и криптографическая схема.

В конце второй эры и начале третьей, внимание ученых сосредоточено на фундаментальных проблемах и, соответственно, на математической области. Можно утверждать в полной мере, что сейчас ученые могут определять и вычислительную область, которая по своей сути обращается на взаимодействие между математическими и криптографическими примитивами. В этом случае, математическая область составляется как бы мощность гомоморфных вычислений, ту ошибку, которая накапливается после каждой операции, а область информационных процессов составляет некий количественный буфер, способность выдерживать эту ошибку. Гомоморфное шифрование имеет непосредсвенную зависимость от математических и криптографических примитивов, отражая таким образом как межуровневую связь, так и связь с различными областями.

1.4 Итоги

Подведём итоги развития гомоморфного шифрования и выделим актуальные направления развития.

1. Вычислительные проблемы
    а) Модульная арифметика
        1) Факторизация
        2) Квадратичные вычеты
        3) Композитные вычеты
        4) Вычеты произвольной степени
        5) Дискретное логарифмирование
        6) Поиск наибольшего делителя
    б) Решетки
        1) Проблема проблема эквивалента среднего/худшего базиса
        2) Прооблема кратчайшего вектора
        3) Аппроксимация среднего вектора
        4) Проблема соседнего вектора
    в) Обучение с ошибками
        1) Обучение с ошибками в пространстве колец
    г) Комбинаторные проблемы
        1) Укладка рюкзака
        2) Subset-sum
        3) Раскраска графа
2. Математические примитивы
    а) Бинарная логика
    б) Пространство остатков целых чисел
    в) Идеалы
    г) Усеченые кольца
    д) Линейные коды
    е) Биллинейные спаривания на эллиптических кривых
3. Криптографические примитивы
    а) Atomic proxy cryptography
        1) Самонастройка (bootstraping)

2) Перешифровка (refleshing)
3) Упаковка шифртекста
4) Пороговое ограничение шифртекста (перелинеаризация)

б) Односторонняя функция
в) Забывчивая передача
г) Защищенные индексы

4. Криптографические схемы
   а) Вычисление функций
      1) Искаженная схема
      2) NC^1-цепи
      3) Формулы 2-DNF
      4) Ациклические графы
   б) Пороговое шифрование
      1) Шифрование атрибутов
      2) Выборочная идентификация
   в) Гомоморфность
      1) Частичная
      2) Ограниченная
      3) Полная
   г) Обфускация
   д) Арифметика больших чисел
   е) Публичный ключ

Глава 2.

2.1 Обобщенные операции над шифртекстом

В криптографической системе можно выделить несколько областей, состоящих из различных уровней. Это некоторые математические примитивы, которые сформированы вокруг сложной вычислительной проблемы, а также криптографические примитивы, которые организуют уровень криптографической схемы.

Для примера выделим обозначенные уровни в криптосистеме RSA. Так, уровень вычислительной проблемы представлен задачей факторизации целых чисел. Уровень математических примитивов представлен операциями возведения в степень по модулю в пространстве целых чисел. Уровень криптографических примитивов составляет такой примитив, как односторонняя функция. Наконец, последний уровень характеризуется протоколом обмена ключами и ассиметричностью (наличием, публичного и секретного ключа).

Условно, что в такой схеме можно провести следующую границу: первые два уровня формируют область математической абстракции, в то время, как последние два уровня формируют область преобразования информации и взаимодействия с ней.

Подобное разделение позволяет описать системы с хэшированием, шифрованием, цифровой подписью или другими соответствующими информационными процессами. Однако, для гомоморфных систем имеет место следующее уточнение.

Гомоморфные свойства можно обозначить, как продукт, принадлежащий одновременно уровнями математических и криптографических примитивов, что означает, что их можно отделить как от низлежащей математической проблемы, так и от криптографической схемы, т. е. выделить уровень вычислительной абстракции.

Попытаемся показать это через определение обобщенных операций. Определим такую операцию над шифртекстом. Известно, что в общем случае операция над шифртекстом может определяться через последовательность некоторых элементарных операций, то есть представлять собой выполнение алгоритма. Такие алгоритмические функции, обозначаемые словами, например, Add и Mult, вызывают соответствующие преобразования со стороны открытого

текста. Определив множество элементов открытого текста $c \in C$ и шифртекста $\psi \in \Psi$, мы можем записать, например:

$$Add\,(\psi_1,\psi_2) \to c_1 + c_2;\ Mult\,(\psi_1,\psi_2) \to {}_1 + {}_2;$$

Набор операций сложения и умножения образует гомоморфную систему шифрования. Обобщая бинарную операцию с множества открытого текста на множество шифртекста, мы можем выделить следующие свойства:

1. Множество открытого текста является подмножеством шифртекста, $C \in \Psi$, и оба множества могут быть разбиты с помощью элементов одних и тех же непересекающихся множеств, образующих множество R. Рассматривая элементы $c \in C$ как элементы группы, элементы $\psi \in \Psi$ являются векторами над элементами множества C.

$$C \in R : \Psi \in R^k; R = R_1 \cup R_2 \cup R_3 \ldots \cup R_N;\ N = |R|\,;$$

2. Операции над шифртекстом и открытым текстом можно определить через одинаковые операции над множеством R.
3. При этом результат операций над шифртекстом оставляет возможность расшифрования и получения октрытого текста на уровне криптографической схемы.

Тогда операция Op является обобщенной, если:

$$Op:\ \psi_1 \odot \psi_2 \to c_1 \odot c_2;$$

$$a,b \in C : a \odot b : \forall R_i \subset R \bigcap C,\ r^i \in R_i : \left[r_a^1 \odot r_b^1\ ; r_a^2 \odot r_b^2; r_a^3 \odot r_b^3; \ldots\right];$$

Например, конгруэнтная криптосистема поддерживает обобщенную гомомофрную операцию сложения по умолчанию, благодаря преобразованиям на множестве идеалов.

На уровне множеств любая криптосистема может быть дополнения обобщенными операциями без нарушения своей структуры до уровня криптографической схемы. На последнем же уровне необходимо разрешить вопрос расшифрования с учетом накапливаемой ошибки. При этом не всякая криптосисема может это позволить.

2.2 Конгруэнтная система шифрования

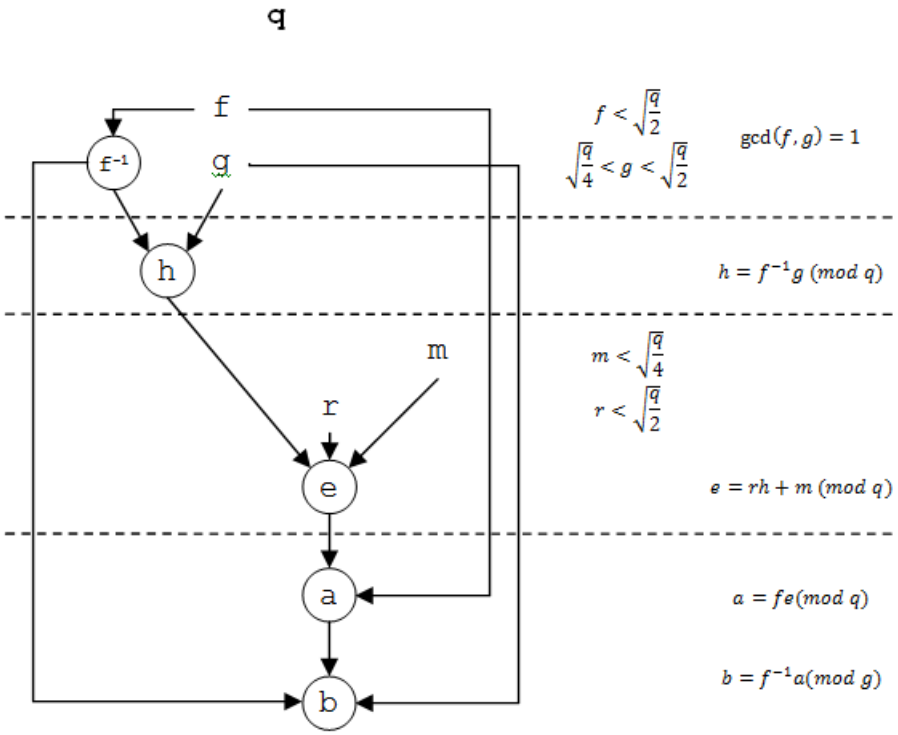

Рисунок 2.1 — Схема конгруентной криптосистемы

Когруэнтая криптосистема описана в [105].

Конгруэнтная криптосистема очень удобна, как начальная модель для рассмотрения. Ее запись можно свести к функции получения расшифрованного сообщения в следующей форме:

$$\pi^* = f\,(\pi,r,q,\mathrm{f},g)\,,\begin{cases}\pi,r,q,\mathrm{f},g \in \mathbb{Z}\\ g < q,\mathrm{f} < \sqrt{q/2}\\ \exists\ \mathrm{f}^{-1}\ mod\ q = \mathrm{f}_q^{-1}\\ gcd(f,g) = 1\end{cases}$$

$$\pi^* = \left(f_g^{-1}\cdot(\mathrm{f}\cdot\psi\ mod\ q)\right)\ mod\ g = \left(\mathrm{f}_g^{-1}\cdot(\mathrm{f}\cdot(r\cdot h+\pi)\ \ mod\ q)\right)\ mod\ g =$$
$$= \left(\mathrm{f}_g^{-1}\cdot\left(\mathrm{f}\cdot\left(r\cdot\left(g\cdot\mathrm{f}_q^{-1}\right)+\pi\right)\ \ mod\ q\right)\right)\ mod\ g;$$

, где ψ – шифртекст, π – сообщение, r – случайное число, q, g, f - параметры системы. Учитывая секретный и публичный ключи, соответственно, равенство

можно перезаписать, как:

$$pk = \left(g \cdot \mathrm{f}_q^{-1}, q\right) = (h, q)\ ,\ sk = (\mathrm{f}, g)$$

$$\begin{aligned}\pi^* &= (f\ (sk) \cdot (sk_1 \cdot (r \cdot pk_1 + \pi)\ \ mod\ pk_2))\ \ mod\ sk_2 = \\ &= f\ ((r \cdot pk_1 + \pi)\ , pk_2, sk, sk_1, sk_2) = f\ (f\ (r \cdot pk_1, \pi)\ , pk_2, sk, sk_1, sk_2) = \\ &= f\ (f\ (\pi, f(r, pk_1))\ , pk_2, sk, sk_1, sk_2) = (f(\pi, u)\ mod\ pk_2)\ \ mod\ sk_2\end{aligned}$$

Наличие публичного и секретного ключа позволяет реализовать систему асимметричной криптографии. К обеим формам записи мы будем приходить, рассматривая и последующие криптосистемы. Такие нотации удобны, так как они показывают "уровневую" структуру криптографических схем, где каждый этап работы соответствует одному или нескольким порядкам оператора приоритета (т. е. скобок). Первая форма описывает криптосистему, раскрывая содержание её параметров на уровне математической записи, в то время как вторая форма описывает более высокий уровень абстракции, раскрывающий содержание криптографической схемы или протокола. Груба говоря, первая форма - эта форма математических примитивов, а вторая форма - это форма криптографических примитивов.

Для конгруэнтной криптосистемы вторую форму записи можно обобщить, как:

$$\begin{aligned}\pi^* = \psi\ mod\ sk_2 = (t\ mod\ pk_2)\ \ mod\ sk_2 = (f(\pi, u)\ mod\ pk_2)\ \ mod\ sk_2 = \\ = (f(\pi, f(r, pk_1))\ mod\ pk_2)\ \ mod\ sk_2\end{aligned}$$

, где $\pi \in \Pi$ - элемент множества открытого текста, $u \in U$ - элемент шумового множества, $r \in R$ - элемент множества случайных значений, $t \in T$ - элемент множества усеченного (редуцированного) шифртекста, $\psi \in \Psi$ - элемент множества шифртекста.

Эта третья форма записи является более специфичной и отображает некоторые преобразования, которые производятся над исходным сообщением. В-частности имеет место следующая карта отображений:

$$\left.\begin{matrix}\Pi \\ \mathrm{R} \to \mathrm{U}\end{matrix}\right\} \to \mathrm{T} \to \Psi$$

$$\Pi \to (\Pi + pk_1 \cdot \mathrm{R} = \mathrm{T}) \to \Psi$$

Покажем на примере конгруэнтной криптосистемы, каким образом её можно ее дополнить, чтобы производить вычисления над зашифрованными сообщениями. Для полей целых чисел при паре взаимно простых значений pk_1 и sk_2 операции умножения и сложения над шифртекстом реализуют гомоморфизм для всех изоморфных пространств, позволяя определить операции над шифртекстом как обобщенные:

$$\begin{aligned}\psi_1 + \psi_2 &= ((\pi_1 + g \cdot r_1) + (\pi_2 + g \cdot r_2)) \ \ mod\ q = \\ &= (\pi_1 + g \cdot r_1 + q \cdot k) + (\pi_1 + g \cdot r_2 + q \cdot k) = \\ &= (\pi_1 + \pi_2) + g \cdot (r_1 + r_2) + q \cdot 2k = ((\pi_1 + \pi_2) + g \cdot (r_1 + r_2)) \ \ mod\ q\end{aligned}$$

$$\begin{aligned}\psi_1 \times \psi_2 &= \psi_1 \cdot \psi_2 \\ &= (\pi_1 + g \cdot r_1) \cdot (\pi_2 + g \cdot r_2) \ \ mod\ q \\ &= (\pi_1 + g \cdot r_1 + q \cdot k) \cdot (\pi_2 + g \cdot r_2 + q \cdot k) \\ &= \pi_1 \cdot \pi_2 + g \cdot \pi_1 \cdot r_2 + q \cdot \pi_1 \cdot k + g \cdot \pi_2 \cdot r_1 + g \cdot g \cdot r_1 r_2 + q \cdot g \cdot r_1 k + q \cdot \pi_2 \cdot k + q \cdot g \cdot k r_2 + q \cdot q \cdot k^2 \\ &= \pi_1 \cdot \pi_2 + g \cdot \pi_1 \cdot r_2 + g \cdot \pi_2 \cdot r_1 + g \cdot g \cdot r_1 r_2 + q \cdot \pi_1 \cdot k + q \cdot \pi_2 \cdot k + q \cdot g \cdot k r_1 + q \cdot g \cdot k r_2 + q \cdot q \cdot k^2 \\ &= (\pi_1 \cdot \pi_2 + g \cdot \pi_1 \cdot r_2 + g \cdot \pi_2 \cdot r_1 + g \cdot g \cdot r_1 r_2) \ \ mod\ q \\ &= (\pi_1 \cdot \pi_2 + g \cdot (\pi_1 \cdot r_2 + \pi_2 \cdot r_1 + g \cdot r_1 r_2)) \ \ mod\ q\end{aligned}$$

Как видно, результаты аддитивной и мультипликативной операций обладают той же формой, что и исходные шифртексты. Из-за монотонно возрастающего значения r, обе операции ведут к накоплению ошибки в пространстве шифртекста. Операции выполняются, пока π не превысит значение g и $t = \pi + g \cdot r$ не превысит значение q. Это можно записать как набор условий для функции вычислений C:

$$C(\psi_1, \psi_2, \ldots, \psi_n) \to \psi_C,\ \pi_C < g,\ \pi_C + g \cdot r_C < q$$

Таким образом, мы можем говорить о некоторой глубине вычислений по сложению и умножению. Однако, точное определение этого понятия, а также количественная оценка несколько затруднительны, при наличии сразу двух независимых условий. Для упрощения можно использовать понятие глубины вычислений с нулевым шумом ($r_C = 0$), глубине вычислений по шуму ($\pi_C = 0$), а также глубине вычислений с нормированными шифртекстом и шумом ($\forall \pi_{1..n} : \pi = 1 \quad \forall r_{1..n} : r = 1$), которое выражается в минимальном количестве операций, которые может выдержать цепочка вычислений C. Кроме этого, также можно использовать отношение мощности множеств:

$$|\Pi| < \frac{|U|}{|R|},\ |T| < |\Psi|$$

Последний вариант представляется наиболее подходящим для оценки глубины вычислений, в особенности, если мощности множеств Π, R и T могут быть выражены друг через друга. Например, если мощности множеств можно получить через публичный и секретный ключи, и эти ключи имеют взаимосвязь, тогда, приняв во внимание, что для повышения криптостойкости за счёт введения вероятностной величины обычно выполняется условие $|\Pi| \ll |U|$, мы можем производить оценку глубины вычислений, рассматривая соотношения мощности шумового множества к множеству шифртекста. Также, оценка глубины вычислений и реализация гомоморфных операций вообще может усложняться в случае негенерализированных операций, так как производные продукты вычислений будут приводить к ещё большему накоплению ошибки. Сами же генерализированные операции представляются лучшим случаем для реализации гомоморфных систем, и, по возможности, в дальнейшем мы будем предполагать именно такие операции и оценивать на их основе глубину вычислений. Таким образом, на основе трёх представленных форм записи, мы можем рассматривать математические свойства, определяющие возможность гомоморфных операций, и криптографические свойства, которые эти операции реализуют. Третья форма записи позволяет рассмотреть общий параметр, связывающий криптографические и гомоморфных свойства системы. В этом плане выбор математического примитивна определяет накопление ошибки в пространстве шифртекста, в том время, как реализация криптографической схемы задаёт некоторый объём, который может выдержать эта ошибка. В основе классической NTRU заложены принципы конгруэнтной криптосистемы. Несмотря на то, что она изначально не использует элементы решетчатых пространств, оценку криптостойкости такой системы можно свести к задаче нахождения кратчайчешго вектора для двумерной векторной решётки.

Криптосистема Джентри, как и другие системы на решетках, может быть сведена к конгруэнтной криптосистеме. Функция шифрования записывается в виде:

$$\psi \leftarrow \pi^* \ mod \ B_J^{pk}$$

Функция расшифровки может быть представлена в виде:

$$\pi \leftarrow \left(\psi \ mod \ B_J^{sk}\right) \ mod \ B_I$$

Как видно для шифрования используется один уровень отображения, в то время как для расшифрования используется два отображения. Базис B_I одновременно включает в себя и случайную составляющую, которая может быть описана распределением D:

$$\pi^* \leftarrow Samp\,(B_I, D, r', \pi')\;;;\; \pi', r' \in \mathbb{Z}$$

Базисы B_I и B_J являются взаимно простыми.

Базовую криптосистему Джентри в соответствии с нашей нотацией можно представить в виде:

$$\pi^* = \Psi \bmod B_I = \left(R \bmod B_J^{sk}\right) \bmod B_I = \left(\left(\pi \bmod B_J^{pk}\right) \bmod B_J^{sk}\right) \bmod B_I$$

В сравнении с записью конгруэнтной криптосистемы, там также можно выделить три уровня. С помощью различных базисов B_J реализуется асимметричная криптосистема. В криптосистеме Джентри первую и вторую записи можно объединить в одну.

Для построения своей криптосистемы Джентри использует “решечатые” пространства в полной мере, а ее криптоанализ, как и в случае с конгруэнтной криптосистемой, можно свести к задаче нахождения кратчайшего вектора. Принимая во внимание общую запись в нашей нотации, это показывает не только то, что криптосистема Джентри является обобщением конгруэнтной криптосисистемы, а конгруэнтная криптосистема является частным случаем криптосистемы Джентри на случай редуцирования размерности “решетчатого” пространства, но и анализ тех частей, из которых она состоит. Для построения такой криптосистемы используется пространство решеток и алгебра над полем идеалов. Причем, нет явной связи между этими двумя частями, что позволяет выдвинуть предположение о независимости построения криптографической и гомоморфной схем.

Общая запись в нашей нотации также указывает на схожие принципы построения с точностью до того, какие уровни раскрытия равенства выбраны на различных этапах для шифрования и расшифрования. Так, обе системы состоят из трех уровней, но в первом случае для конгруэнтной криптосистемы используются первых два уровня в шифровании и последний в рашифровании, во втором случае первый уровень и последние два, соответственно. Все это, совместно

с замечанием Джентри о независимости процесса придания свойства недетерменированности криптографической системе и выводами в пункте выше, о независимости построения криптографической и гомоморфной схем, позволяет выдвинуть следующее предположение. Таким криптосистемам присущ общий процесс последовательности независимых отображений для множества открытого текста, “шумового множества” и множества шифртекста, который можно представить в следующем виде:

$$\begin{array}{ccccccc} \Pi & \to & L & & & & \\ & & + & \to & T & \to & \Psi \\ R & \to & U & & & & \end{array}$$

Рассмотрим подробнее все обозначенные множества. Множества Π и R по сути являются одномерными множествами, которые “сэмплируются” в множества L и U, соответственно. Множество случайных значений R задает вероятностную криптосистему. Преимущество такой системы состоит в том, что детерминированная система позволяет злоумышленнику использовать оператор сравнения, наличие которого значительно снижает криптостойкость таких систем, особенно для компьютеров с квантовой архитектурой. Подобного недостатка лишены вероятностные (недетерминированные) криптосистемы, в которых одному сообщению может соответствовать несколько различных шифртекстов. В общем виде преобразование $\Pi \to$ T добавляет некоторый случайный элемент. Можно выделить два элементарных подхода к объединению случайного элемента и исходного сообщения: с отбрасыванием, либо с выделением остаточной части. В первом случае $L > U$, во втором $L < U$. Далее происходит отображение имеющее вид односторонней функции.

(Теорема А.А.)Такие преобразования обладают рядом важных свойств. Во-первых, преобразование $\Pi \to$ T является биективным, отображая каждый элемент Π в подмножества $T^* \subset$ T. Если мощность множества $|\Pi| < \frac{|U|}{|R|}$,то $|\Pi| < |T^*|$, и подмножества T^* не пересекаются, т. е. $\forall T_k^*, T_l^* \subset T$, $k \neq l$: $T_k^* \cap T_l^* = \varnothing$. Если $|\Pi| = (\frac{|U|}{|R|} - 1)$, то $|\Pi| = |T^*|$, и подмножества T^* также образуют множество T, т. е. $\bigcup_{\forall T^* \subset T} T^* = T$. Это означает, что при правильно выбранном параметре секретного ключа, множество Π отображается в непересекающиеся множества и на множестве R можно задать функцию равномерного распределения D. И если преобразование $T \to \Psi$ криптостойко (т. е. единствен-

ная возможная атака – это перебор), выполнение условий, описанных выше, не дает коллизий на всем преобразовании $\Pi \to T > \Psi$.

Каким образом мы можем учесть гомоморфные операции? Можно вспомнить о том, что криптосистема Джентри и конгруэнтная криптосистема реализуют векторное пространство. Для него можно учесть следующие условия, которые относятся к накоплению ошибки. Во-первых, это теорема о неравенстве треугольника:

$$\|\psi_1 + \psi_2\| \leqslant \|\psi_1\| + \|\psi_2\|$$

а также, как следствие гомоморфизма:

$$\|t_1 + t_2\| \leqslant \|t_1\| + \|t_2\|\,,\ \|r_1 + r_2\| \leqslant \|r_1\| + \|r_2\|\,,\ \|\pi_1 + \pi_2\| \leqslant \|\pi_1\| + \|\pi_2\|$$

Для умножения выполняется следующее условие [Джентри, с. 81]:

$$\|\psi_1 \times \psi_2\| \leqslant \gamma_{mult} \cdot \|\psi_1\| \cdot \|\psi_2\|$$

, где γ_{mult} зависит только от используемого кольца. Как видно, вектора способны выдерживать аддитивную ошибку, и для аддитивной операции возможно выполнение требования теоремы А.А. Однако нельзя исключить накопление мультипликативной ошибки, для которой мы можем требовать, чтобы $|T| \,?\, |\Psi|$. Таким образом, мы можем выдвинуть некоторое предположение о синтезе гомоморфной системы шифрования. С одной стороны, требуется, чтобы для $\Pi \to T^*$: $\bigcup_{\forall T^* \subset T} T^* = T$ и $\forall T_k^*, T_l^* \subset T,\ k \neq l : T_k^* \cap T_l^* = \varnothing$. С другой стороны, для гомоморфности по сложению и умножений последнее условие не может выполняться в связи с необходимостью глубины вычислений, для которой $|T| \,?\, |\Psi|$.

Как будет показано ниже, использование в конструкции множеств идеалов, придаст отображению $\Pi \to T > \Psi$ свойства идеального шифра, для которого Ψ не выдает никакой информации о T и Π.

Кроме этого, криптосистема Джентри для выделения сообщения π использует отбрасывание незначащей части, содержащей случайную величину, которое реализовано в виде операций взятия по модулю. Для конгруэнтной криптосистемы используется взятие остатка по модулю. Оба подхода также подтверждают два способа, которые могут быть использованы, чтобы ввести случайную величину, представленные выше для U и L.

Выше было сказано о том, что когруэнтную криптосистему и криптосистему Джентри можно обобщить, покажем, как это можно сделать. Вторая запись для конгруэнтной криптосистемы имеет вид:

$$\begin{aligned}\pi^* &= \psi \ mod \ sk_2 \\ &= \left(t \ mod \ pk_2\right) \ mod \ sk_2 \\ &= \left(f(\pi,u) \ mod \ pk_2\right) \ mod \ sk_2 \\ &= \left(f(\pi,f(r,pk_1)) \ mod \ pk_2\right) \ mod \ sk_2\end{aligned}$$

Не конкретизируя производимые операции, мы можем записать:

$$\begin{aligned}\pi^* &= \psi \ mod \ sk_2 \\ &= \left(t \ mod \ pk_2\right) \ mod \ sk_2 \\ &= \left(f(\pi,u) \ mod \ pk_2\right) \ mod \ sk_2 \\ &= f\left(f\left(\pi,f\left(r,pk_1\right)\right), \ sk_2,pk_2\right)\end{aligned}$$

, где $pk = \left(g \cdot \mathrm{f}_q^{-1},q\right) = (h,q)$, $sk = (\mathrm{f},g)$. Мы можем вспомнить определение публичного и секретного ключа. Публичный ключ используется для шифрования, секретный ключ для шифрования. Но тогда q также входит в секретный ключ, как видно из записи выше. Следовательно, мы можем записать:

$$sk = (f,g,q)\,; pk = \left(f\left(sk\right),sk_3\right) = f\left(sk\right);$$

$$\begin{aligned}\pi^* &= f\left(f\left(\pi,f\left(r,pk_1\right)\right), \ sk_2,pk_2\right) \\ &= f\left(f\left(\pi,f\left(r,f(sk)\right)\right), \ sk_2,sk_3\right) \\ &= f\left(f\left(\pi,f\left(r,f(sk)\right)\right), \ sk\right)\end{aligned}$$

Как видно, публичный ключ в данной записи можно выразить через секретный ключ, в частности реализуя одностороннюю функцию. Для криптосистемы Джентри ситуация аналогичная:

$$\begin{aligned}\pi^* &= f\left(\psi,B_J^{sk},B_I\right) = f\left(f\left(\mathrm{L},B_J^{pk}\right),B_J^{sk},B_I\right) \\ &= f\left(f\left(Samp\left(B_I,\pi\right),B_J^{pk}\right),B_J^{sk},B_I\right) = f\left(f\left(Samp\left(B_I,\pi\right),B_J^{pk}\right),B_J^{sk},B_I\right) \\ &= f\left(f\left(Samp\left(B_I,\pi\right),IdealGen^{pk}\left(B_I,r\right)\right),IdealGen^{sk}(B_I,r),B_I\right)\end{aligned}$$

Как видно, B_I является искомым базисом, через который выражает секретный ключ $sk = \left(IdealGen^{sk}\left(B_I,r\right),B_I,r\right)$ и публичный ключ $pk = \left(IdealGen^{pk}\left(B_I,r\right),B_I\right) = f(f\left(sk\right),B_I)$

$$\pi^* = f\left(f\left(Samp\left(B_I,\pi\right),f(r,f\left(sk\right)\right)\right),sk\right)$$

Отличие криптосистемы Джентри состоит в том, что функция отображения множества Π в множество L является более сложной, изменяя также размерность множества. То есть, обе криптосистемы поддаются более общей форме записи, в виде:

$$\pi^* = f\left(\psi,sk\right) = f\left(f\left(l,u\right),sk\right) = f\left(f\left(f\left(\pi\right),f\left(r,f\left(sk\right)\right)\right),sk\right)$$

, где $\pi,\pi^* \in \Pi$, $\psi \in \Psi$, $r \in \mathrm{R}$. Таким образом, мы показали, что публичный ключ имеет связь с секретным ключом, и в дальнейшем мы будем использовать эту связь, чтобы упростить оценку глубины вычислений. Для конструкции публичного ключа применяется односторонняя функция на секретном ключе.

Джентри рассматривает применение идеалов в векторном пространстве как наилучший случай для реализации гомоморфных схем. Прежде чем мы проведем конкретные реализации гомоморфных криптосистем, важно рассмотреть наши модели на уровне идеалов. Используемую нотацию с применением идеалов можно перезаписать, принимая во внимание основную теорему арифметики о делении. Тогда последовательность отображений в конгруэнтной криптосистеме позволяет получить шифртекст в виде:

$$\Psi = \Pi + g \cdot R + q \cdot M$$

Очевидно, что в данном случае отображения представляют собой отображения множеств идеалов, а именно:

$$\Pi \to [\Pi] \to [\Pi + g \cdot R]$$

Такие преобразования обладают рядом важных свойств. Во-первых, как уже было сказано выше, при правильно выбранном параметре g, множество Π отображается в непересекающиеся множества и на множестве R можно задать функцию равномерного распределения.

Во-вторых, это позволяет получить максимальное расстояние (расстояние Хемминга) между шифртекстами. Можно показать, что при достаточно большой выборке это расстояние будет стремиться к расстоянию между двумя шифртекстами, как если бы они были получены из исходных сообщений без

добавления случайной величины. В этом плане подобные преобразования реализуют принципиальную неразличимость, был ли получен шифртекст $\psi \in \Psi$ напрямую из Π, $\Pi \to \Psi$, или он был получен, как $\Pi > \mathrm{R} > \Psi$ (для соответствующей функции сэмплирования). Если параметры подобраны правильно, то есть $\pi < g$ и $t < q$, то на множестве идеалов $\Pi > \mathrm{R}$ (т. е. $\Pi > [\Pi]$) равномерно и не имеет коллизий и при том, если $[\Pi] \to [\Pi + g \cdot \mathrm{R}]$ криптографически стойко, то шифртекст на множестве Ψ не выдает никакой информации о сообщении на множестве Π, то есть реализует свойства идеального шифра. Следовательно, использование идеалов на всем преобразовании, т. е. $\Pi > [\Pi] > [\Pi + g \cdot \mathrm{R}]$ также криптостойко. Таким образом, применение идеалов в дополнение к теореме об отсутствии коллизий А.А дает неразличимость шифртекста и открытого текста.

Что касается гомоморфных операций, то наличие алгебры в кольце множества Ψ является гомоморфизмом для исходного множества Π. Как уже было сказано выше, можно выделить два простейших подхода к реализации этого гомоморфизма; более сложные могут быть их комбинацией. Для идеалов эти два подхода могут быть реализованы с помощью основной теоремы арифметики о делении. Для $u \in U$:

$$u = a \cdot g + b$$

В первом $a = r$, $b = \pi$ варианте “шумовой текст” имеет вид:
$u = \pi + g \cdot r$, где $\pi < g$

$$U = \Pi + [R]$$

Тогда сообщение π можно получить, выполнив операцию взятия по модулю g, т. е. найдя остаток от деления:

$$\pi = u \bmod g$$

Во втором случае наоборот, $a = \pi$, $b = r$ и “шумовой текст” имеет вид:
$u = r + g \cdot \pi$, где $r < g$

$$U = [c] + R$$

В этом случае сообщение π получается путем отбрасывания “шума” от u:

$$\pi = |u| = u - (u \bmod g)$$

Более сложные способы можно обозначать через задание известной функции распределения d:

$$\Pi\, d \to\ U \to \Psi$$

Разница в двух упомянутных способах различает некоторым "буфером" ошибки. В первом случае корректная расшифровка возможна, пока: $r < g$ и $(r + g \cdot \pi) < q$,

$$|r| < |g| < \frac{|\Psi|}{|\Pi|}$$

Во втором случае, пока: $\pi < g$ и $(\pi + g \cdot r) < q$,

$$|\pi| < |g| < \frac{|\Psi|}{|R|}$$

В случае использования главных идеалов для q и g для второго случая генереализировнные операции в кольце идеалов примут вид:

$$\begin{aligned}
\psi_1 + \psi_2 &= \left[\pi_1 + g \cdot r_1\right] + \left[\pi_2 + g \cdot r_2\right] \\
&= \left(\pi_1 + g \cdot r_1 + q \cdot k\right) + \left(\pi_1 + g \cdot r_1 + q \cdot k\right) \\
&= \\
&= (\pi_1 + \pi_2) + g \cdot (r_1 + r_2) + q \cdot 2k \\
&= \left[(\pi_1 + \pi_2) + g \cdot (r_1 + r_2)\right]
\end{aligned}$$

$$\begin{aligned}
\psi_1 \times \psi_2 &= \left[\pi_1 + g \cdot r_1\right] \times \left[\pi_2 + g \cdot r_2\right] \\
&= \left(\pi_1 + g \cdot r_1 + q \cdot k\right) \times \left(\pi_2 + g \cdot r_2 + q \cdot k\right) \\
&= \\
&= \pi_1 \times \pi_2 + g \times \pi_1 \cdot r_2 + q \times \pi_1 \cdot k + g \times \pi_2 \cdot r_1 + g \times g \cdot r_1 r_2 \\
&\quad + q \times g \cdot r_1 k + +q \times \pi_2 \cdot k + q \times g \cdot k r_2 + q \times q \cdot k^2 \\
&= \pi_1 \times \pi_2 + g \times \pi_1 \cdot r_2 + g \times \pi_2 \cdot r_1 + g \times g \cdot r_1 r_2 + +q \times \pi_1 \cdot k \\
&\quad + q \times \pi_2 \cdot k + q \times g \cdot k r_1 + q \times g \cdot k r_2 + q \times q \cdot k^2 \\
&= \\
&= \left[\pi_1 \times \pi_2 + g \times \pi_1 \cdot r_2 + g \times \pi_2 \cdot r_1 + g \times g \cdot r_1 r_2\right] \\
&= \\
&= \left[\pi_1 \times \pi_2 + g \times (\pi_1 \cdot r_2 + \pi_2 \cdot r_1 + g \cdot r_1 r_2)\right]
\end{aligned}$$

Как видно, мультипликативный и аддитивный продукты операции имеют ту же форму, что и исходный шифртекст. Под знаком $\times$ определено векторное умножение, под знаком $\cdot$ определено скалярное умножение.

Список литературы

1. Коробейников, А. Г. Математические основы криптологии / А. Г. Коробейников, Ю. А. Гатчин. — 2004.
2. Diffie, W. New directions in cryptography / W. Diffie, M. Hellman // IEEE transactions on Information Theory. — 1976. — Т. 22, № 6. — С. 644—654.
3. FIPS, P. 46-3. Data Encryption Standard (DES) / P. FIPS // National Institute of Standards and Technology. — 1999. — Т. 25, № 10. — С. 1—22.
4. Landau, S. Designing Cryptography for the New Century. / S. Landau // Commun. ACM. — 2000. — Т. 43, № 5. — С. 115—120.
5. Kelsey, J. Yarrow-160: Notes on the design and analysis of the yarrow cryptographic pseudorandom number generator / J. Kelsey, B. Schneier, N. Ferguson // International Workshop on Selected Areas in Cryptography. — Springer. 1999. — С. 13—33.
6. Müller, S. Linux random number generator—a new approach / S. Müller.
7. Biryukov, A. State of the art in lightweight symmetric cryptography / A. Biryukov, L. P. Perrin. — 2017.
8. Rivest, R. L. A method for obtaining digital signatures and public-key cryptosystems / R. L. Rivest, A. Shamir, L. Adleman // Communications of the ACM. — 1978. — Т. 21, № 2. — С. 120—126.
9. Shamir, A. How to share a secret / A. Shamir // Communications of the ACM. — 1979. — Т. 22, № 11. — С. 612—613.
10. Lamport, L. Constructing digital signatures from a one-way function : тех. отч. / L. Lamport ; Technical Report CSL-98, SRI International Palo Alto. — 1979.
11. Adleman, L. On taking roots in finite fields / L. Adleman, K. Manders, G. Miller // 18th Annual Symposium on Foundations of Computer Science (sfcs 1977). — IEEE. 1977. — С. 175—178.
12. Karp, R. M. Reducibility among combinatorial problems / R. M. Karp // Complexity of computer computations. — Springer, 1972. — С. 85—103.

13. Brassard, G. A note on the complexity of cryptography (corresp.) / G. Brassard // IEEE Transactions on information Theory. — 1979. — Т. 25, № 2. — С. 232—233.

14. On data banks and privacy homomorphisms / R. L. Rivest, L. Adleman, M. L. Dertouzos [и др.] // Foundations of secure computation. — 1978. — Т. 4, № 11. — С. 169—180.

15. Caupolicań Peralta, R. Three results in number theory and cryptography: A new algorithm to compute square roots modulo a prime number; On the bit complexity of the discrete logarithm; A framework for the study of cryptoprotocols / R. Caupolicań Peralta. — University of California, Berkeley, 1985.

16. Miller, V. S. Use of elliptic curves in cryptography / V. S. Miller // Conference on the theory and application of cryptographic techniques. — Springer. 1985. — С. 417—426.

17. Goldwasser, S. New directions in cryptography: twenty some years later (or cryptograpy and complexity theory: a match made in heaven) / S. Goldwasser // Proceedings 38th Annual Symposium on Foundations of Computer Science. — IEEE. 1997. — С. 314—324.

18. Kilian, J. Founding crytpography on oblivious transfer / J. Kilian // Proceedings of the twentieth annual ACM symposium on Theory of computing. — ACM. 1988. — С. 20—31.

19. Even, S. A randomized protocol for signing contracts / S. Even, O. Goldreich, A. Lempel // Communications of the ACM. — 1985. — Т. 28, № 6. — С. 637—647.

20. Cohen, J. D. A robust and verifiable cryptographically secure election scheme / J. D. Cohen, M. J. Fischer. — Yale University. Department of Computer Science, 1985.

21. Benaloh, J. Verifiable secret-ballot elections [Ph. D. Thesis] / J. Benaloh // Yale University. — 1987.

22. Blum, M. How to exchange (secret) keys / M. Blum // Proceedings of the fifteenth annual ACM symposium on Theory of computing. — ACM. 1983. — С. 440—447.

23. Blum, M. Coin flipping by telephone / M. Blum // Proc. of COMPCON, IEEE, 1982. — 1982.

24. Feldman, P. A practical scheme for non-interactive verifiable secret sharing / P. Feldman // 28th Annual Symposium on Foundations of Computer Science (sfcs 1987). — IEEE. 1987. — С. 427—438.

25. Shamir, A. IP= PSPACE (interactive proof= polynomial space) / A. Shamir // Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science. — IEEE. 1990. — С. 11—15.

26. Brickell, E. F. On privacy homomorphisms / E. F. Brickell, Y. Yacobi // Workshop on the Theory and Application of of Cryptographic Techniques. — Springer. 1987. — С. 117—125.

27. Goldwasser, S. Probabilistic encryption & how to play mental poker keeping secret all partial information / S. Goldwasser, S. Micali // Proceedings of the fourteenth annual ACM symposium on Theory of computing. — ACM. 1982. — С. 365—377.

28. Goldreich, O. Foundations of Cryptography:(fragments of a Book / O. Goldreich. — 1995.

29. Micali, S. CS proofs / S. Micali // Proceedings 35th Annual Symposium on Foundations of Computer Science. — IEEE. 1994. — С. 436—453.

30. Goldwasser, S. Multi party computations: past and present / S. Goldwasser // Proceedings of the sixteenth annual ACM symposium on Principles of distributed computing. — ACM. 1997. — С. 1—6.

31. Chor, B. Computationally private information retrieval / B. Chor, N. Gilboa // Journal of the ACM. — Citeseer. 1997.

32. Okamoto, T. A new public-key cryptosystem as secure as factoring / T. Okamoto, S. Uchiyama // International conference on the theory and applications of cryptographic techniques. — Springer. 1998. — С. 308—318.

33. Paillier, P. Public-key cryptosystems based on composite degree residuosity classes / P. Paillier // International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 1999. — С. 223—238.

34. Sander, T. Non-interactive cryptocomputing for nc/sup 1 / T. Sander, A. Young, M. Yung // 40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039). — IEEE. 1999. — С. 554—566.

35. Blaze, M. Divertible protocols and atomic proxy cryptography / M. Blaze, G. Bleumer, M. Strauss // International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 1998. — С. 127—144.

36. Sahai, A. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security / A. Sahai // 40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039). — IEEE. 1999. — С. 543—553.

37. Dolev, D. Non-Malleable Cryptography. STOC'91 / D. Dolev, C. Dwork, M. Naor. — 1991.

38. Pointcheval, D. Chosen-ciphertext security for any one-way cryptosystem / D. Pointcheval // International Workshop on Public Key Cryptography. — Springer. 2000. — С. 129—146.

39. Feigenbaum, J. Random-self-reducibility of complete sets / J. Feigenbaum, L. Fortnow // SIAM Journal on Computing. — 1993. — Т. 22, № 5. — С. 994—1005.

40. Fellows, M. Combinatorial cryptosystems galore! / M. Fellows, N. Koblitz // Contemporary Mathematics. — 1994. — Т. 168. — С. 51—51.

41. Boneh, D. Algorithms for black-box fields and their application to cryptography / D. Boneh, R. J. Lipton // Annual International Cryptology Conference. — Springer. 1996. — С. 283—297.

42. Ajtai, M. Generating hard instances of lattice problems / M. Ajtai // Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. — ACM. 1996. — С. 99—108.

43. Goldreich, O. Public-key cryptosystems from lattice reduction problems / O. Goldreich, S. Goldwasser, S. Halevi // Annual International Cryptology Conference. — Springer. 1997. — С. 112—131.

44. Hoffstein, J. NTRU: A ring-based public key cryptosystem / J. Hoffstein, J. Pipher, J. H. Silverman // International Algorithmic Number Theory Symposium. — Springer. 1998. — С. 267—288.

45. Dent, A. W. A designer's guide to KEMs / A. W. Dent // IMA International Conference on Cryptography and Coding. — Springer. 2003. — С. 133—151.

46. Katz, J. Bridging game theory and cryptography: Recent results and future directions / J. Katz // Theory of Cryptography Conference. — Springer. 2008. — С. 251—272.

47. Heindl, R. New directions in multivariate public key cryptography / R. Heindl. — 2009.

48. Monico, C. J. Semirings and semigroup actions in public-key cryptography : дис. ... канд. / Monico Christopher J. — University of Notre Dame Notre Dame, 2002.

49. Déchene, I. Generalized Jacobians in cryptography. Т. 68 / I. Déchene. — 2006.

50. Peikert, C. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices / C. Peikert, A. Rosen // Theory of Cryptography Conference. — Springer. 2006. — С. 145—166.

51. Peikert, C. Lattices that admit logarithmic worst-case to average-case connection factors / C. Peikert, A. Rosen // Proceedings of the thirty-ninth annual ACM symposium on Theory of computing. — ACM. 2007. — С. 478—487.

52. Micciancio, D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions / D. Micciancio // The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings. — IEEE. 2002. — С. 356—365.

53. Kawachi, A. Multi-bit cryptosystems based on lattice problems / A. Kawachi, K. Tanaka, K. Xagawa // International Workshop on Public Key Cryptography. — Springer. 2007. — С. 315—329.

54. Choosing NTRUEncrypt parameters in light of combined lattice reduction and MITM approaches / P. S. Hirschhorn [и др.] // International Conference on Applied Cryptography and Network Security. — Springer. 2009. — С. 437—455.

55. Howgrave-Graham, N. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU / N. Howgrave-Graham // Annual International Cryptology Conference. — Springer. 2007. — С. 150—169.

56. Boneh, D. Evaluating 2-DNF formulas on ciphertexts / D. Boneh, E.-J. Goh, K. Nissim // Theory of Cryptography Conference. — Springer. 2005. — С. 325—341.

57. Rivest, R. L. A method for obtaining digital signatures and public-key cryptosystems / R. L. Rivest, A. Shamir, L. Adleman // Communications of the ACM. — 1978. — Т. 21, № 2. — С. 120—126.

58. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms / T. ElGamal // IEEE transactions on information theory. — 1985. — Т. 31, № 4. — С. 469—472.

59. Lyubashevsky, V. Generalized compact knapsacks are collision resistant / V. Lyubashevsky, D. Micciancio // International Colloquium on Automata, Languages, and Programming. — Springer. 2006. — С. 144—155.

60. Micciancio, D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions / D. Micciancio // computational complexity. — 2007. — Т. 16, № 4. — С. 365—411.

61. Hellman, M. E. An overview of public key cryptography / M. E. Hellman // IEEE Communications Magazine. — 2002. — Т. 40, № 5. — С. 42—49.

62. Barreno, M. A. The future of cryptography under quantum computers / M. A. Barreno // Dartmouth College Computer Science Technical Reports. — 2002.

63. Melchor, C. A. Lattice-based homomorphic encryption of vector spaces / C. A. Melchor, G. Castagnos, P. Gaborit // 2008 IEEE International Symposium on Information Theory. — IEEE. 2008. — С. 1858—1862.

64. Damgård, I. A length-flexible threshold cryptosystem with applications / I. Damgård, M. Jurik // Australasian Conference on Information Security and Privacy. — Springer. 2003. — С. 350—364.

65. Armknecht, F. A New Approach for Algebraically Homomorphic Encryption. / F. Armknecht, A.-R. Sadeghi // IACR Cryptology ePrint Archive. — 2008. — Т. 2008. — С. 422.

66. Ishai, Y. Evaluating branching programs on encrypted data / Y. Ishai, A. Paskin // Theory of Cryptography Conference. — Springer. 2007. — С. 575—594.

67. Gentry, C. A fully homomorphic encryption scheme. T. 20 / C. Gentry, D. Boneh. — Stanford University Stanford, 2009.

68. Fully homomorphic encryption over the integers / M. Van Dijk [и др.] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2010. — С. 24—43.

69. On the (im) possibility of obfuscating programs / B. Barak [и др.] // Annual International Cryptology Conference. — Springer. 2001. — С. 1—18.

70. Dijk, M. van. Interval obfuscation / M. van Dijk, S. Devadas // as an MIT-CSAIL Technical Report in. — 2009.

71. Regev, O. Lattice-based cryptography / O. Regev // Annual International Cryptology Conference. — Springer. 2006. — С. 131—141.

72. Using fully homomorphic hybrid encryption to minimize non-interative zero-knowledge proofs / C. Gentry [и др.] // Journal of Cryptology. — 2015. — Т. 28, № 4. — С. 820—843.

73. Ajtai, M. Generating hard instances of lattice problems / M. Ajtai // Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. — ACM. 1996. — С. 99—108.

74. Goldreich, O. Public-key cryptosystems from lattice reduction problems / O. Goldreich, S. Goldwasser, S. Halevi // Annual International Cryptology Conference. — Springer. 1997. — С. 112—131.

75. Hoffstein, J. Invertibility in truncated polynomial rings : тех. отч. / J. Hoffstein, J. Silverman ; Technical report, NTRU Cryptosystems, October 1998. Report. — 1998.

76. Gentry, C. Computing arbitrary functions of encrypted data / C. Gentry // Communications of the ACM. — 2010. — Т. 53, № 3. — С. 97—105.

77. Smart, N. P. Fully homomorphic encryption with relatively small key and ciphertext sizes / N. P. Smart, F. Vercauteren // International Workshop on Public Key Cryptography. — Springer. 2010. — С. 420—443.

78. Mikuš, M. Experiments with the plaintext space in Gentry's somewhat homomorphic scheme / M. Mikuš // Tatra Mountains Mathematical Publications. — 2012. — Т. 53, № 1. — С. 147—154.

79. Regev, O. On lattices, learning with errors, random linear codes, and cryptography / O. Regev // Journal of the ACM (JACM). — 2009. — Т. 56, № 6. — С. 34.

80. Lyubashevsky, V. A toolkit for ring-LWE cryptography / V. Lyubashevsky, C. Peikert, O. Regev // Annual International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2013. — С. 35—54.

81. Brakerski, Z. Fully homomorphic encryption from ring-LWE and security for key dependent messages / Z. Brakerski, V. Vaikuntanathan // Annual cryptology conference. — Springer. 2011. — С. 505—524.

82. Brakerski, Z. Efficient fully homomorphic encryption from (standard) LWE / Z. Brakerski, V. Vaikuntanathan // SIAM Journal on Computing. — 2014. — Т. 43, № 2. — С. 831—871.

83. Brakerski, Z. (Leveled) fully homomorphic encryption without bootstrapping / Z. Brakerski, C. Gentry, V. Vaikuntanathan // ACM Transactions on Computation Theory (TOCT). — 2014. — Т. 6, № 3. — С. 13.

84. Gentry, C. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based / C. Gentry, A. Sahai, B. Waters // Annual Cryptology Conference. — Springer. 2013. — С. 75—92.

85. Cheon, J. H. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero / J. H. Cheon, J. Jeong, C. Lee // LMS Journal of Computation and Mathematics. — 2016. — Т. 19, A. — С. 255—266.

86. Fully homomorphic encryption using ideal lattices. / C. Gentry [и др.] // Stoc. Т. 9. — 2009. — С. 169—178.

87. Coppersmith, D. Lattice attacks on NTRU / D. Coppersmith, A. Shamir // International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 1997. — С. 52—61.

88. Gentry, C. Key recovery and message attacks on NTRU-composite / C. Gentry // International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2001. — С. 182—194.

89. Ajtai, M. A public-key cryptosystem with worst-case/average-case equivalence / M. Ajtai, C. Dwork // STOC. Т. 97. — Citeseer. 1997. — С. 284—293.

90. Micciancio, D. Improved cryptographic hash functions with worst-case/average-case connection / D. Micciancio // Proceedings of the thiry-fourth annual ACM symposium on Theory of computing. — ACM. 2002. — С. 609—618.

91. Peikert, C. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices / C. Peikert, A. Rosen // Theory of Cryptography Conference. — Springer. 2006. — С. 145—166.

92. Gentry, C. Trapdoors for hard lattices and new cryptographic constructions / C. Gentry, C. Peikert, V. Vaikuntanathan // Proceedings of the fortieth annual ACM symposium on Theory of computing. — ACM. 2008. — С. 197—206.

93. Lyubashevsky, V. On ideal lattices and learning with errors over rings / V. Lyubashevsky, C. Peikert, O. Regev // Annual International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2010. — С. 1—23.

94. Micciancio, D. Lattice-based cryptography / D. Micciancio // Encyclopedia of Cryptography and Security. — 2011. — С. 713—715.

95. Performance Improvements and a Baseline Parameter Generation Algorithm for NTRUSign. / J. Hoffstein [и др.] // IACR Cryptology ePrint Archive. — 2005. — Т. 2005. — С. 274.

96. Classic McEliece: conservative code-based cryptography / D. J. Bernstein [и др.] // NIST submissions. — 2017.

97. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer / P. W. Shor // SIAM review. — 1999. — Т. 41, № 2. — С. 303—332.

98. Practical lattice-based cryptography: NTRUEncrypt and NTRUSign / J. Hoffstein [и др.] // The LLL Algorithm. — Springer, 2009. — С. 349—390.

99. Multiparty computation with low communication, computation and interaction via threshold FHE / G. Asharov [и др.] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2012. — С. 483—501.

100. Gentry, C. Homomorphic evaluation of the AES circuit / C. Gentry, S. Halevi, N. P. Smart // Annual Cryptology Conference. — Springer. 2012. — С. 850—867.

101. Fast cryptography in genus 2 / J. W. Bos [и др.] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2013. — С. 194—210.

102. Brakerski, Z. Fully homomorphic encryption without modulus switching from classical GapSVP / Z. Brakerski // Annual Cryptology Conference. — Springer. 2012. — С. 868—886.

103. Stehlé, D. Making NTRU as secure as worst-case problems over ideal lattices / D. Stehlé, R. Steinfeld // Annual International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2011. — С. 27—47.

104. Gentry, C. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based / C. Gentry, A. Sahai, B. Waters // Annual Cryptology Conference. — Springer. 2013. — С. 75—92.

105. An introduction to mathematical cryptography. Т. 1 / J. Hoffstein [и др.]. — Springer, 2008.