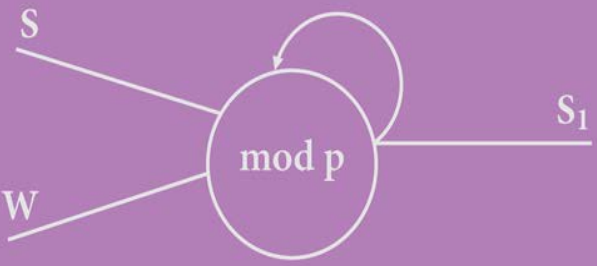
ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ И СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ В КРИПТОГРАФИИ



ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ И СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ В КРИПТОГРАФИИ

МОСКВА
ФИЗМАТЛИТ ®
2012

УДК 681.3.067
ББК 32.973-018.2
П76

Авторский коллектив:
Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н.,
Лавриненко А.В.

Применение искусственных нейронных сетей и системы остаточных классов в криптографии. — М.: ФИЗМАТЛИТ, 2012. — 280 с. — ISBN 978-5-9221-1386-1.

В монографии изложены идеи искусственных нейронных сетей и системы остаточных классов в их приложении к криптографии, причем рассмотрены различные типы искусственных нейронных сетей. Представлены результаты научных исследований за последнее десятилетие в области защиты информации с применением элементов искусственного интеллекта и модулярной арифметики. Изложенные результаты представляют значительный интерес для современных разработчиков нейросетевых криптосистем на базе системы остаточных классов. Приведена библиография работ по применению нейрокомпьютеров для решения задач теории графов.

Для студентов, бакалавров, магистров, аспирантов, научных работников и специалистов в области информационной безопасности, занимающихся вопросами применения искусственных нейронных сетей и системы остаточных классов в криптографии.

ISBN 978-5-9221-1386-1

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Причина написания этой монографии состоит в том, что в последнее время появилось много статей зарубежных авторов с изложением нового подхода к применению искусственных нейронных сетей и системы остаточных классов в криптографических преобразованиях, с одной стороны, и обострилась проблема внедрения рассматриваемых идей в практику, с другой стороны.

Криптографические преобразования мотивированы множеством сложных математических проблем, которые связаны с вычислительной алгеброй (конечные поля, конечные группы, теория колец), теорией чисел, теорией вероятности, логикой, диофантовой сложностью, алгебраической геометрией и другими. Эффективность современных криптосистем зависит от решения сложных в вычислительном отношении проблем. Вычисления не могут быть закончены за полиномиальное время вследствие наличия проблемы разложения числа на множители, вычисления дискретного логарифма на эллиптических кривых, проблемы ранца, решения нелинейной системы алгебраических уравнений и др.

В этой работе для решения проблем криптографии предлагается применение искусственных нейронных сетей, которые могут быть использованы для аппроксимации и обучения задачам из области криптографии.

Главная цель криптографии состоит в том, чтобы дать возможность двум или нескольким людям общаться через незащищенный канал таким образом, чтобы оппонент не мог понять того, о чем идет речь.

Искусственные нейронные сети базируются на свойствах биологических систем, а более определенно, на законах работы человеческого мозга. Формально, искусственные нейронные сети представляют собой распределенные процессоры с массовым параллелизмом, реализованные на базе простых процессоров (нейронов), которые имеют естественную склонность к сохранению знаний, основанных на опыте, и делают доступными их использование. Это напоминает работу мозга по двум причинам: во-первых, знания приобретаются сетью от среды с помощью процесса обучения и, во-вторых, силы межнейронных связей, называемые синаптическими весами, используются для хранения приобретенных знаний. Каждый искусственный нейрон характеризуется отношением вход–выход и осуществляет локальное вычисление. Выход любого нейрона определяется его входными и выходными характеристиками, взаимосвязью с другими нейронами и, возможно, с внешними входами. Функциональные возможности искусственных нейронных сетей определяются их топологией, алгоритмами обучения и характеристиками их нейронов. Вычислительная мощность нейронных сетей определяется их параллельной распределенной структурой и свойственной им способностью адаптации к определенным задачам, к обучению и обобщению. Эти характеристики позволяют искусственным нейронным сетям решать сложные задачи криптографии.

Развитие распределенных систем обработки данных выдвинуло на первый план задачу информационной безопасности системы в целом — состояние защищенности всех процессов обработки, хранения и передачи информации в системе. Криптография предоставляет большой набор локальных и распределенных средств обеспечения безопасности работы системы, таких как электронная цифровая подпись, идентификация и аутентификация абонентов, безопасное хранение ключей и многое

другое. В решении этих проблем находит свое место использование искусственных нейронных сетей.

Известно, что искусственные нейронные сети прямого распространения с одним скрытым слоем имеют нижнюю границу степени аппроксимации любой функции. Данная граница может быть повышена, если используется более чем один скрытый слой. Это обстоятельство позволяет внедрить мощный вычислительный инструмент в дискретных алгебраических структурах, появляющихся в криптологии.

Монография состоит из девяти глав и одного приложения.

Глава 1 «Общие вопросы криптографии и нейросетевые технологии» посвящена общим вопросам применения нейросетевых технологий в криптографии. Представлены общие вопросы применения нейронных сетей в системах криптографической защиты информации. Описана криптосистема, в которой хранение информации проводится в устойчивых состояниях нейронных сетей, а представление информации — в произвольных состояниях нейронных сетей. Представлена реализация интерактивных протоколов идентификации абонентов с применением нейросетевых технологий. Описаны нейросетевые модели пролонгированной безопасности, основанные на периодическом пространственном разделении секрета. Приводятся результаты анализа криптостойкости подобной нейронной криптографии.

Глава 2 «Модификации структур нейронных сетей в криптографии» посвящена описанию и модификациям структур нейронных сетей, применяемых в криптографии. Рассматриваются различные типы структур нейронных сетей в решении криптографических задач: 1) нейронные сети с задержкой; 2) хаотические нейронные сети.

Глава 3 «Взаимодействующие нейронные сети в криптографии» посвящена направлению в криптографии, связанному с применением так называемых взаимодействующих нейронных сетей, которые в процессе функционирования становятся зеркальными отображениями друг друга. Вместо обычной процедуры пересылки ключа перед пересылкой сообщения могут использоваться две нейронные сети, использующие в качестве ключа свои скрытые весовые коэффициенты.

Глава 4 «Нейросетевая криптография с открытым ключом» представляет материалы по нейронной криптографии с открытым ключом. Применение нейросетевых технологий здесь эффективно в том случае, когда стоимость вычислительной системы значительно возрастает при достижении необходимого времени решения задачи. Здесь нейросетевые технологии применяются для шифрования, дешифрования и формирования секретного ключа. Недостаток, заключающийся в отсутствии прозрачности нейронной сети, ограничивает возможности использования нейросетевых технологий. В данной главе, в частности, описана нейросетевая криптографическая система с открытым ключом на базе скрытых линейных преобразований. Приведено исследование производительности нейронных сетей применительно к проблемам криптографии. Отмечаются особенности реализации криптосистемы с открытым ключом и цифровой подписи на базе нейронных сетей.

Глава 5 «Нейросетевые технологии в стеганографии» посвящена проблеме защиты цифровых изображений. Описан хаотичный алгоритм кодирования, криптоаналитические исследования и результаты экспериментов. Представлено описание методологии SCAN, которая является пространственной методологией доступа. Рассматривается частный случай так называемой Q-тронной нейронной сети для реализации визуальной криптосистемы. Представлены алгоритмы генерации искусственных текстур, использующие нейронные сети частной структуры

Глава 6 «Нейросетевые технологии в системах аутентификации пользователей информации» описывает возможные схемы аутентификации пользователей по паролям для различных архитектур вычислительных систем с использованием нейросетевых

технологий. Представлены тесты на базе нейронных сетей для качественной оценки алгоритмов дайджеста сообщений.

Глава 7 «Нейросетевые алгоритмы решения математических задач в криптографии» представляет новое направление в вычислительной математике — нейроматематику, связанную с решением сложных математических задач в нейросетевом логическом базисе. Рассмотрены нейросетевые алгоритмы решения задач сложения по модулю 2 для вычисления функции проверки четности. Описаны нейросетевые алгоритмы решения задачи разложения чисел на простые множители, эффективного модульного возведения в степень с использованием генетических алгоритмов, разрешения коллизий и др.

В главе 8 «Нейросетевые алгоритмы генерации случайных чисел в криптографических системах» представлены псевдослучайные генераторы на базе нейронных сетей различной структуры — системы с богатыми свойствами нелинейности динамики. Отдельно рассматривается клеточная нейронная сеть как гистерезисный хаотический генератор. Представлены материалы по количественной оценке качества генераторов случайных чисел и показаны количественные преимущества нейросетевых генераторов.

В главе 9 «Блочные шифры и нейросетевые технологии» представлены материалы по реализации элементарных операций блочного шифрования с помощью нейросетевых технологий. Описано применение рекуррентных нейронных сетей для решения задачи проектирования симметричных шифров.

В приложении представлена библиография работ по применению нейросетевых технологий для решения задач теории графов.

Данная монография рассчитана на широкий круг читателей: студентов, бакалавров, магистров, преподавателей, инженеров, аспирантов, научных работников и профессионалов в области защиты информации и криптографии.

Глава 1

ОБЩИЕ ВОПРОСЫ КРИПТОГРАФИИ И НЕЙРОСЕТЕВЫЕ ТЕХНОЛОГИИ

1.1. Нейронные сети в системах криптографической защиты информации

Развитие распределенных систем обработки данных выдвинуло на первый план задачу информационной безопасности системы в целом, а именно состояние защищенности всех процессов обработки, хранения и передачи информации в системе [1.1]. Для обеспечения безопасности работы системы криптография предоставляет большой набор локальных и распределенных средств, таких как электронная цифровая подпись, идентификации и аутентификации абонентов, коды аутентификации, безопасное хранение ключей и многое другое. Ключ — это главный секрет во всем процессе шифрования. Как показано в [1.2], применение ключей связано с производством (генерацией), запоминанием, безопасным хранением, распределением и уничтожением. В данном разделе рассматривается вопрос безопасного хранения ключей с использованием принципа пороговых криптосистем. В [1.3] для хранения ключей предлагается справочник с открытыми ключами всех корреспондентов, который помещается на общедоступном сервере. Сервер обеспечивает допуск в сеть зарегистрированных пользователей, которых может быть больше двух. Иногда для этих целей используется центр распределения ключей, который осуществляет взаимодействие с одним или несколькими участниками сеанса.

Все криптографические преобразования связаны с выполнением операций сложения, умножения и вычитания с элементами кольца вычетов z_m. Стойкость ряда современных криптосистем определяется сложностью теоретико-числовых задач и величиной чисел, участвующих в вычислениях. Так, при использовании схемы шифрования RSA используются довольно большие числа, порядка 250–300 десятичных разрядов [1.3].

Возможности современных ЭВМ имеют определенные границы, поэтому при вычислениях необходимо разбивать имеющуюся последовательность на блоки ограниченной длины и шифровать каждый блок отдельно. Кроме того, стандартное математическое обеспечение ЭВМ не позволяет перемножать числа размером более 65 десятичных знаков, которые необходимо обрабатывать при криптографических методах защиты данных. Известно, что большие числа всегда можно разбить на меньшие блоки, с которыми компьютер может оперировать так же, как мы оперируем с цифрами, когда проводим вычисления вручную на бумаге, но для этого нужны специальные программы. Для вычислений с большими числами созданы и получили достаточно широкое распространение даже специальные языки программирования [1.3], например PARI и UBASIC.

Известны и другие алгоритмы умножения очень больших чисел, когда одно большое простое число заменяется несколькими меньшими простыми числами. Так, при умножении двух целых чисел, состоящих из 10 000 бит, в цифровой вычислительной машине с длиной слова 24 бита использовались три простых числа $p_1 = 6\,946\,817$, $p_2 = 7\,340\,033$, $p_3 = 7\,667\,713$ и при этом умножение двух различных целых чисел

выполнено в два раза быстрее, чем умножение этих чисел при использовании большого простого числа [1.4].

Наибольшее быстродействие может быть достигнуто путем применения нейроускорителей, использующих возможность массовых параллельных вычислений при выполнении различного рода преобразований [1.5]. Для современных ЭВМ с их стандартным математическим обеспечением предлагается использовать для вычислений с большими числами нейроускорители, функционирующие в системе остаточных классов (СОК).

Наиболее уязвимыми местами распределенной вычислительной системы являются именно места хранения секретной ключевой информации [1.2, 1.3]. Перспективным направлением в настоящее время являются системы активной безопасности [1.6], которые включают в себя: периодическое обновление секретной информации путем смены паролей и ключей, использование одноразовых паролей и другие приемы, а также пространственное разделение секретной информации. Системы активной безопасности служат для защиты от долговременных атак противника.

Использование криптографического разделения секрета позволяет конструировать ключ из отдельных элементов данных, имеющихся у различных участников или абонентов распределенной вычислительной системы. Секретный ключ восстанавливается путем сбора этих элементов, количество которых достаточно для восстановления исходного ключа. Протоколы аутентификации (называемые также протоколами идентификации) являются частью информационных систем, которые работают в компьютерной сети и обеспечивают доступ к данным. У идентификатора системы имеется список всех пользователей вместе с выделенным каждому из них набором полномочий, на основе которых осуществляется разграничение доступа к ресурсам системы. В протоколе может быть более двух участников.

Рассмотрим принцип восстановления ключа в пороговых криптосистемах. Пусть K — ключ, который требуется сохранить в распределенной системе обработки информации, состоит из n компонентов. Под компонентами подразумеваются аппаратные средства: ЭВМ, программное обеспечение, данные и пользователи. При этом требуется, чтобы любые L пользователей из тех n $(n > L)$, которые получили информацию о ключе, могли бы вместе восстановить ключ, но никакая группа из $L-1$ пользователей или менее не могла этого сделать.

Для решения этой задачи сформулируем условия выбора оснований СОК, которые распределены между пользователями криптосистемы. Принцип выбора оснований СОК приведен в [1.4]. Выберем упорядоченный вектор оснований СОК $q < p_1 < p_2 < \ldots < p_n$. Числа p_i для $i = 1, 2, \ldots, n$ взаимно простые, т. е. $(p_i, p_j) = 1$ для $i \neq j$. Каждому пользователю криптосистемы приписывается свое большое простое число p_i $(i = 1, 2, \ldots, n)$. Выберем $q > K$, такое что $(q, p_i) = 1$ для всех $i = 1, 2, \ldots, n$. Произведение L наименьших чисел p_i должно быть больше, чем произведение q и $L-1$ наибольших чисел p_i, т. е. $p_1 p_2 \ldots p_L > q p_{n-L+2} p_{n-L+3} \ldots p_n$. Если $R = p_1 p_2 \ldots p_L$, тогда (R/q) должно быть больше, чем произведение любых $L-1$ чисел p_i.

Выберем случайное число r в интервале $\left[0, \left((R/q) - 1\right)\right]$ и вычислим $K' = K + rq$, чтобы K' попало в интервал $[0, R-1]$. Для восстановления ключа K пользователю необходима информация в виде r и $K_i \equiv K' \bmod p_i$, $i = 1, 2, \ldots, n$.

Центр распределения ключей генерирует по идентификатору, поступившему от любого пользователя, случайное число r и вычисляет K'. Если один из пользователей сети хочет узнать ключ сеанса связи каких-либо пользователей, то он может получить его на основании r и K', полученных от центра распределения ключей. Информация, полученная от центра распределения ключей, должна быть аутентифицирована с помощью его собственного ключа. Передающая и принима-

ющая сторона восстанавливают ключ, который знают только они. Для этой цели центр распределения ключей по запросу пользователя вычисляет и передает числа r и K', по которым пользователь определяет ключ сеанса связи, используемый только в одном случае. Схема организации сети для передачи информации о ключе показана на рис. 1.1.

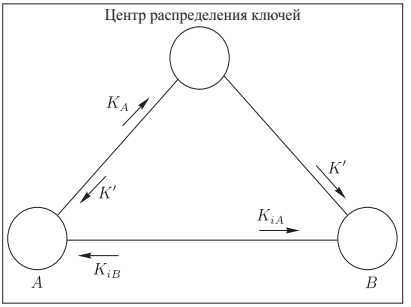


Рис. 1.1. Схема организации сети для передачи информации

Предположим, что A инициирует диалог с B. Пользователи A и B имеют ключи, которые называются соответственно K_A и K_B и которые они используют для связи с центром распределения ключей. По совокупности этих ключей с помощью службы аутентификации центра распределения ключей устанавливается их подлинность. Перед сеансом связи A и B пользователь A устанавливает связь с центром распределения ключей, используя для этого идентификатор и ключ K_A. На рис. 1.1 эта связь показана стрелкой с названием K_A. По защищенным каналам центр распределения ключей передает пользователям A и B числа r и K', выбранные случайно (на рис. 1.1 показано стрелкой с буквой K'). Принятые сообщения A и B используют для вычисления значений K_{iA} и K_{iB}, которыми они обмениваются между собой. По числам K_{iA} и K_{iB} пользователи A и B восстанавливают ключ K. Теперь оба пользователя обеспечены ключом сеанса связи для предстоящего диалога.

В условиях быстро меняющейся ситуации информация о ключах распределяется через сеть, что требует такой же организации центра распределения ключей, который необходим для формирования информации о ключах сеанса связи. Итак, информация об используемых ключах защищена и в явном виде по каналам связи не передается.

Пример. Для простоты вычислений будем использовать небольшие числа, хотя на практике применяются очень большие числа. Пусть ключ $K = 9$, число пользователей сети $L = 2$, число всех пользователей $n = 3$. Выберем взаимно простые числа $q = 13$, $p_1 = 17$, $p_2 = 19$, $p_3 = 23$. Проверим условие $R = p_1 p_2 > q p_3 = 17 \cdot 19 > 13 \cdot 23 = 323 > 299$, условие выполняется. Выберем случайное число r в интервале $\left[0,\ \left(\frac{p_1 p_2}{q} - 1\right)\right] = [0,\ 23]$, например $r = 2$. Найдем $K' = K + qr = 9 + 2 \cdot 13 = 35$. Распределяемые числа r и K' передаются всем пользователям, которые определяются как $K_i \equiv K'_i \bmod p_i$, $i = 1,\ 2,\ \ldots, n$. Итак, $K_1 \equiv 35 \bmod 17 = 1$, $K_2 \equiv 35 \bmod 19 = 16$, $K_3 \equiv 35 \bmod 23 = 12$. По любым двум из этих чисел можно восстановить ключ K, а в общем случае количество выборок определяется сочетанием L из n. Например,

для K_1 и K_3 имеем $K_1 = 1 \pmod{17}$, $K_3 = 12 \pmod{23}$. На основании китайской теоремы об остатках восстановим и определим ключ

$$K = K' - qr. \tag{1.1}$$

Используя метод ортогональных базисов [1.5], восстановим ключ K. Вначале определим $K' \equiv K_1 B_1 + K_3 B_3$, где B_1 и B_3 — ортогональные базисы. По определению ортогональные базисы могут быть представлены в виде: $B_1 = m_1 p_3$, $B_3 = m_3 p_1$ где m_1 и m_3 — веса базисов, соответственно B_1 и B_3. Причем m_1 и m_3 выбираются из сравнений $m_1 p_3 \equiv 1 \bmod p_1$, $m_3 p_1 \equiv 1 \bmod p_3$. Ввиду малости величин оснований решим сравнения путем подбора m_1 и m_3, $m_1 = 3$, $m_3 = 19$. Тогда, $B_1 = 3 \cdot 23 = 69$, $B_3 = 19 \cdot 17 = 323$, $K' = 1 \cdot 69 + 12 \cdot 323 \equiv 3945 \bmod 391 = 35$. Отсюда $K = 35 - 2 \cdot 13 = 9$. Таким образом, восстановленный ключ $K = 9$.

На практике используются длинные криптографические ключи, что приводит к решению задач повышенной размерности, эффективное решение которых можно осуществить с использованием нейросетевых систем, синтезируемых на основе нейроускорителей [1.8], которые представляют собой совокупность нейронных сетей (НС) конечного кольца [1.9] и обычных арифметических элементов, выполняющих арифметические операции.

В архитектуре нейронной сети для восстановления криптографического ключа (рис. 1.2), использованы НС конечного кольца [1.10] и подсеть с арифметическими нейронами. Входной слой разбит на две группы по n' и n'' нейронов.

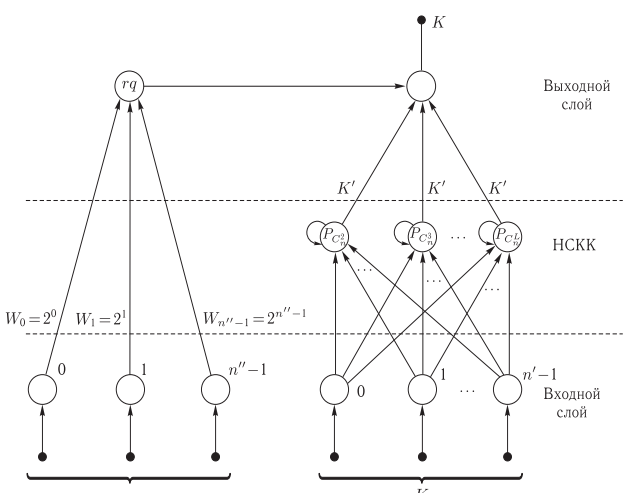


Рис. 1.2. Архитектура НС для восстановления криптографического ключа

Группа с n' нейронами используется для сбора входов K_i, а группа с n'' — для сбора входов r. Синаптические веса первой группы n' равны $W_i P_{C_n^j} = B_{C_n^L}$, где $L = 2, 3, \ldots, n-1$; $j \in \{2, 3, \ldots, L\}$; $L < n$; C_n^L — число сочетаний из n по L. Синаптические веса для второй группы n'' равны $W_i = 2^i$, где $i = 0 \ldots n'' - 1$. Нейрокомпьютер конечного кольца реализует вычислительную модель $K' \equiv \sum_{i=2}^{L} K_i B_{C_n^L} \bmod P_{C_n^L}$. Синаптические веса выходного слоя равны 1.

Синтезированная таким образом НС может быть реализована на ПЛИС Xilinx, она обеспечивает высокую эффективность при решении задач повышенной размерности, что невозможно сделать на обычных ЭВМ. Рассмотренный метод разделения данных является одним из наиболее перспективных средств безопасного хранения криптографических ключей в распределенных вычислительных сетях. Кроме того, этот метод является составной частью новых систем криптографической защиты данных, а именно систем активной безопасности, разработка которых считается самым актуальным направлением современной криптографии. Системы активной безопасности служат для защиты от долговременных атак противника и призваны обеспечить безопасное функционирование распределенных вычислительных сетей при условии ее защищенности в течение длительного времени работы.

1.2. Нейронная криптосистема

Ниже представлена новая криптосистема, использующая нейронные сети [1.11]. Сообщение m в незашифрованном тексте можно рассматривать как устойчивое состояние нейронной сети. Зашифрованная строка сообщения m в зашифрованном тексте является произвольным состоянием, которое приведет нейронную сеть в аттрактор, определяемый оригинальным сообщением m. Процедура шифрования $C = \mathrm{E}(m)$ рассматривает сообщение m из открытого текста как аттрактор нейронной сети и генерирует состояние C случайным образом так долго, как этого состояния C требуется для приведения к правильному аттрактору m. Процедура дешифрования $m = D(C) = D(E(m))$ регенерирует аттрактор нейронной сети из состояний C, содержащихся в зашифрованном тексте.

Особенность предложенной нейронной криптосистемы заключается в хранении информации в устойчивых состояниях нейронных сетей, а представление информации — в произвольных состояниях нейронных сетей.

Поскольку компьютерные сети приобрели популярность, все больше и больше секретной информации передается через каналы связи, в которых возможно прослушивание и перехват. Например, банковские счета постоянно передаются между различными городами. Для хранения такой чувствительной к защите информации используется много алгоритмов шифрования. Криптография используется для передачи информации только через ненадежный канал.

Предлагаемая нейронная криптосистема основана на теории динамических систем [1.14, 1.15]. Идея заключается в хранении информации в устойчивых состояниях динамических систем [1.12, 1.13]. В частности, для реализации криптосистемы здесь используется нейронная сеть. Данная нейронная сеть, прежде всего, описывается нейронным режимом $p \subseteq X$ системы. Такой режим p также называется состоянием нейронной сети. Все такие состояния вместе формируют пространство H(X), называемое пространством состояний. Кроме того, эволюция нейронной сети в своем пространстве состояний точно определяется правилом перехода.

Спецификация нейронной сети включает определение пространства состояний и набор правил (матрица синаптических связей, вектор порогов и функции активации нейронов) для движения в пространстве состояний. Большинство эволюций

нейронных сетей являются необратимыми. Орбита системы — это траектория в ее пространстве состояний. Со временем орбиты соединяются, и после большого числа шагов орбиты, начинающие в различных начальных состояниях, сосредотачиваются возле «аттракторов». Эти аттракторы обычно содержат только очень малую часть возможных состояний. Эволюция сети к аттрактору из произвольного начального состояния реализует функцию шифрования данных.

Строка p в открытом тексте может рассматриваться как устойчивое состояние нейронной сети. Зашифрованная строка в шифротексте является произвольным состоянием, которое приведет сеть к аттрактору, определяемому по оригинальной строке p. Процедура шифрования обрабатывает строку в открытом тексте как аттрактор сети и генерирует состояние случайно так долго, как этого требуется для приведения состояния к правильному аттрактору. Объединение таких состояний формирует шифротекст. Процесс дешифрования заключается в генерации аттракторов сети из состояний, содержащихся в шифротексте.

Хорошо известно, что при разбиении ключа длины L, если проблема разбиения может быть сокращена до NP-проблемы, исчерпывающий поиск имеет временную сложность $O(2^L)$. В нейронной криптосистеме, если размер нейронной сети равен L, то исчерпывающий поиск должен иметь дело с более чем 2^L случаями, т. е. он имеет дело со следующим числом случаев:

$$N = 2^{L^3},$$

если используются только аттракторы точек. Если используются сети с цикличными аттракторами малого периода, то пространство ключей должно быть намного больше. Для многих случаев это преимущество достигается без увеличения времени вычислений и сложности пространства.

Если для взлома системы используется перечисляющий поиск, то намного сложнее взломать наши новые криптосистемы с L нейронами, из-за их более высокой временной сложности. Отсюда следует, что наши системы лучше систем с ключами. Однако остается открытый вопрос: можно ли сократить проблему взлома нейронной криптосистемы до NP-задачи?

Алгоритмы для шифрования и дешифрования сделаны открытыми. В секрете будет держаться определение нейронной сети. По сравнению с ключевыми системами длина ключа подобна числу нейронов в сети, и сам ключ подобен определению нейронной сети. Поскольку нейронные сети обрабатывают информацию параллельно, то этот подход является эффективным. Временная сложность взлома наших новых криптосистем зависит от типа нейронных сетей. Как взломать новые криптосистемы, кратко обсуждается ниже. Представлено несколько других преимуществ нейронной криптосистемы. Также даны алгоритмы шифрования и дешифрования и пример моделирования. В п. 1.2.1 предлагаются идеи шифрования данных с использованием нейронных сетей. В п. 1.2.2 дано сравнение нашей системы с криптосистемами, использующими ключи, с выделением преимуществ нашей системы. Пример шифрования дан в п. 1.2.3.

1.2.1. Кодирование данных. Сохранением строки в аттракторе нейронной сети можно зашифровать данные: строка в открытом тексте есть аттрактор, любые состояния сети, которые приводят к правильным аттракторам, шифруют аттракторы. Можно зашифровать строку p из открытого текста, соответствующую аттрактору сети, путем сохранения состояния q сети, которое приведет нейронную сеть к р.

Пусть X будет полным метрическим пространством [1.13]. Строка — это компактное подмножество X. Все возможные строки вместе формируют пространство, называемое пространством данных $H(X)$. Нейронная сеть состоит из нейронного

пространства, которое один к одному соответствует $H(X)$ вместе с отображением. Если сеть имеет k аттракторов

$$P = \{p_1, p_2, \ldots, p_k\},$$

то пространство $H(X)$ разделяется на k подмножеств:

$$H(X) = D_1 \bigcup D_2 \bigcup \ldots \bigcup D_k.$$

Пусть $q \in D_i$ будет произвольным состоянием, тогда эволюция сети с q в качестве начальной точки приведет к аттрактору p_i.

Мы можем определить отображение F как

$$F\colon H(X) \to P$$

или

$$F(q) = p_i, \quad q \in D_i.$$

Процесс восстановления строки $p \in P$ из любого начального состояния сети, $q \in \in H(X)$, называется проблемой дешифрования.

Задав строку $p \in P$ состояния сети, можно найти q такое, чтобы

$$q = F^{-1}(p).$$

Процесс получения точки $q \in H(X)$ из $p \in P$ называется задачей шифрования.

Идею хранения информации в точке притяжения системы можно легко обобщить на хранение информации в сетях с цикличными аттракторами. Таким образом, можно использовать сети с цикличными аттракторами, следовательно использовать в описываемом алгоритме почти все нейронные сети.

Алгоритм шифрования содержит следующие этапы

1) создание частичного списка аттракторов;
2) отношение каждой базовой строки к одному или более аттракторам;
3) раскладывание открытого текста на базовые строки: $\{p_1, p_2, \ldots, p_k\}$;
4) While (не все p_i расшифрованы) do
   произвольно сгенерировать u;
   while (u не приводит к p_i) do
   произвольно сгенерировать другую u;
   end while;
   соотнести u с q_i;
   end while;
5) получение шифротекста:
$$\{q_1, q_2, \ldots, q_k\};$$

Пример использования этого алгоритма для шифрования открытого текста дан в п. 1.2.3.

Алгоритм дешифрования, соответствующий вышеупомянутому алгоритму шифрования:

1) while (не все q_i дешифрованы) do
   проследить аттрактор p_i с q_i как начальный режим;
   end while;
2) преобразование $\{p_1, p_2, \ldots, p_k\}$ в оригинальный открытый текст.

1.2.2. Обсуждение. В современной криптографии всегда предполагается, что противнику известен криптографический алгоритм. Ключ для дешифрования или ключи для шифрования и дешифрования должны держаться в секрете, чтобы неавторизованный пользователь не смог использовать известные алгоритмы.

Криптосистема включает одну процедуру для шифрования и одну для дешифрования. Формально дешифрование существующих криптосистем включает описания для сообщения, ключа, пространства шифротекстов и функции шифрования и дешифрования.

Знание ключа шифрования позволяет зашифровать любые сообщения из пространства сообщений, когда знание ключа дешифрования позволяет восстановить сообщение из его зашифрованной формы. Таким образом, между функциями шифрования и дешифрования существует следующая связь: M — это пространство сообщения, E и D — функции шифрования и дешифрования,

$$m = D(E(m)), \quad m \in M.$$

Нападающий (криптоаналитик) пытается нарушить конфиденциальность, например путем восстановления общего секретного ключа (симметричный случай) или ключа дешифрования (ассиметричный случай). Чтобы предотвратить взлом (криптоанализ), требуется высокая сложность вычисления ключа, даже когда нападающему известны открытый текст P и зашифрованный текст C.

Для предотвращения быстрого взлома криптосистемы задача взлома ключа должна сократиться до NP-задачи. Поскольку не было доказано, что NP $= P$, временная сложность для задачи из NP-класса предполагается выше, чем P, и временная сложность определяется по алгоритму исчерпывающего поиска. Следовательно, на исчерпывающий последовательный поиск должно затрачиваться много времени. Пусть длина ключа будет L, тогда существует 2^L вариантов. Ключ длиной 56 бит даст пространство ключей 2^{56}.

Однако когда много процессоров производят параллельный поиск, задача может быть решена быстрее. Алгоритмы взлома ключа относятся к тем алгоритмам, которые можно очень легко преобразовать в параллельный алгоритм с очень высокой эффективностью. Можно разработать для этой цели и специальную архитектуру. Поскольку скорость является линейной, параллельная временная сложность равна результату деления последовательной временной сложности на число процессоров.

Подводя итоги, можно отметить, что если ключ имеет длину L и если проблема взлома ключа может быть сведена к NP-задаче, то исчерпывающий поиск должен иметь дело с 2^L ключами.

Функция шифрования E и функция дешифрования D даны ниже. Предполагается, что нападающий знает алгоритм. В секрете же держится используемая нейронная сеть. Следующая теорема (теорема Абу-Мустафы и Джакьюса) о нейронной сети показывает преимущество описываемого подхода, если требуется исчерпывающий поиск.

Теорема 1 (теорема Абу-Мустафы и Джакьюса, 1985 г.). Пусть $|\mathrm{X}| = L$, т. е. X имеет L элементов: $x = \{0, 1, 2, \ldots, L-1\}$, тогда существует

$$N = 2^{L^3}$$

сетей Хопфилда.

Спецификация сети будет храниться в секрете. Как показывает вышеупомянутая теорема, существует несколько спецификаций, число которых намного больше, чем систем с открытым или общим ключом, в предположении, что длина ключа и мощность пространства X равны. Конечно, мощность X может быть произвольной, так же как и длина ключа может быть любым числом.

Докажем, что представленная криптосистема может быть лучше, чем системы, использующие ключи. Есть два основных преимущества.

Во-первых, если используется исчерпывающий перебор, то он займет 2^M проверок, где $M = L^3$, а L — это мощность пространства X. В системах, использующих ключи, он занимает только 2^L проверок, где L — это длина ключа. Мощность X может быть любым положительным целым числом, как и в случае длины ключа.

Во-вторых, отображение шифрования

$$C = E(P)$$

не является уникальным. Существует экспоненциально растущее число путей для отображения открытого текста в шифротекст при выбранной сети. Следовательно, даже когда нападающий будет знать открытый текст P и его шифрованный текст C, это не сильно ему поможет, так как следующая передача того же открытого текста P будет иметь совершенно другой шифротекст. Мы покажем это в следующей части. Данная особенность представлена в следующей теореме.

Теорема 2. Пусть $x = \{0, 1, 2, \ldots, L-1\}$. Пусть выбрана сеть и она используется для кодирования n символов. Тогда максимальное число шифротекстов для открытого текста равно

$$\left(\frac{2R}{n}\right)^m,$$

где m — число строк в открытом тексте.

Доказательство. Точки в $H(X)$ представляются n символами. В оптимальном случае, каждый символ представлен равным количеством точек, т. е. каждый символ имеет $|H(X)|/n$ вариантов. Пусть открытый текст содержит m символов, тогда его можно представить одним из $(|H(X)|/n)^m$ вариантов, что и требовалось доказать.

Эта теорема показывает, что при выбранной сети отображение из открытого текста P в шифротекст C не является уникальным. Тот же открытый текст P можно пропустить через канал один миллиард раз. В каждом случае шифротекст будет другим. Нейронную сеть следует заменить задолго до того, как шифротекст того же открытого текста повторится. Таким образом, шифротекст открытого текста почти всегда новый, когда он передается через канал связи. Следовательно, предполагая, что проверка ключа выполняется за одну операцию, проверка сети займет экспоненциально большое число операций.

В итоге, криптосистема является отказоустойчивой и может быть легко реализована.

Предполагается, что алгоритм известен. Поэтому, чтобы взломать систему, нужно найти сеть, используемую при шифровании.

А. Взлом системы без взлома «ключа». Отображение для шифрования

$$C = E(P)$$

не является уникальным. Когда сеть выбрана, существует экспоненциально много путей для отображения открытого текста в шифротекст. Следовательно, знание нападающим и открытого текста P и его шифротекста C ему не поможет, так как последующая передача того же открытого текста P будет иметь совершенно другой шифротекст.

В. Взлом «ключа». Пусть $|X| = L$, где X определено в п. 1.2.2. Существует

$$O\left(2^{L^3}\right)$$

нейронных сетей, которые можно выбрать. Можно последовательно проверять каждую сеть.

Когда сеть выбрана, необходимо проверить все возможные шифротексты для данного открытого текста. Число шифротекстов для данного открытого текста растет как экспонента от длины открытого текста. Поиск займет больше времени, чем для системы на базе ключа.

Таким образом, мы оставляем открытым вопрос: может ли проблема взлома нейронной сети быть уменьшена до NP-проблемы?

1.2.3. Пример моделирования. Предположим, мы хотим зашифровать открытый текст «LIU», который задан в формате ASCII (рис. 1.3).

Символ	ASCII код
L	0100 1100
I	0100 0111
U	0101 0101

Рис. 1.3. Пример открытого текста «LIU» [1.11]

Для простоты, пусть $X = \{0, 1, 2, 3, 4\}$ и состояния обозначены как

$$00000 = 0, \quad 00001 = 1, \ldots,$$
$$11110 = 30, \quad 11111 = 31.$$

Предположим, после численного моделирования сети, существование орбит в пространстве состояний (рис. 1.4).

$$14, 2, 3 \to 7 \to 7$$
$$5 \to 15 \to 7 \to 7$$

$$8 \to 4 \to 11 \to 6 \to 6$$
$$10 \to 6 \to 6$$

$$9 \to 12 \to 13 \to 13$$
$$1 \to 13 \to 13$$

$$16 \to 0 \to 0$$

$$30, 21, 19 \to 23$$
$$21 \to 31 \to 23 \to 23$$

$$24 \to 20 \to 27 \to 22 \to 22$$
$$26 \to 22 \to 22$$

$$25 \to 28 \to 29 \to 29$$
$$17 \to 29 \to 29$$

Рис. 1.4. Орбиты нейронной сети в пространстве состояний [1.11]

Второй шаг алгоритма шифрования заключается в выборе базовых строк. Можно выбрать 0 и 1 как базовые строки. Можно выбрать $0000, 0001, \ldots, 1111$ как базовые строки. Мы можем даже выбрать все ASCII-коды или другие коды как базовые строки. Здесь мы произвольно выбираем набор, изображенный на рис. 1.5, вместе с присваиванием аттрактора, где длинную строку 0100 подбираем первой.

Базовая строка	Присвоенный аттрактор
00	7
01	6
10	13,29
11	23
0100	22

Рис. 1.5. Произвольное присваивание каждой базовой строки одному или более аттрактору [1.11]

Символ	Базовая строка
L	22 23 7
I	22 6 23
U	6 6 6 6

Рис. 1.6. Декомпозиция открытого текста «LIU» на аттракторы [1.11]

На третьем шаге открытый текст преобразуется в набор базовых строк. Это также набор аттракторов. Набор аттракторов для открытого текста «LIU YING», в нашем примере на рис. 1.6, записывается как

22 23 7 22 6 23 6 6 6 6.

На четвертом шаге алгоритма шифруются аттракторы. На рис. 1.7 представлено несколько возможных шифротекстов. Существует много возможных состояний для каждого аттрактора. В результате, есть много разных способов представления одного и того же открытого текста.

1.2.4. Заключение. Выше представлена новая криптосистема. В данной схеме открытый текст является набором аттракторов нейронных сетей. Они зашифрованы в набор произвольных состояний. Преимущество новой системы заключается в повышенной безопасности данных и простоте реализации. Идея шифрования заключается в хранении строки p в аттракторе сети. Тогда зашифрованная строка p в шифротексте есть произвольное состояние динамической системы, которое приводит систему к p (рис. 1.7).

27 23 14	22 8 30	6 11 8 4
20 30 7	27 4 18	11 10 4 8
22 21 2	20 6 23	6 4 8 6
24 31 15	14 11 23	10 11 4 6
26 19 3	22 10 19	11 6 10 8
24 18 5	26 4 31	6 4 4 10

Рис. 1.7. Шесть из многих возможных шифротекстов «LIU», где 0 означает 00000, 1 означает 00001, ... , 31 означает 11111 [1.11]

1.3. Нейросетевые модели пролонгированной безопасности

Основным элементом системы шифрования является секретный ключ, генерации, хранению, обновлению и уничтожению которого предъявляются повышенные требования безопасности [1.24]. Наиболее перспективным методом управления ключами является метод активной безопасности, который базируется на периодическом обновлении ключа, одноразовых паролях и пространственном разделении секрета [1.35]. Системы активной безопасности являются средством противодействия активному (мобильному) противнику, который за определенное время может «взломать» серверы, число которых определяется структурой доступа пороговой схемы (ПС). При этом предполагается, что смена секрета произойдет в момент времени, когда противник успел скомпрометировать $(k-1)$ ключ системы разделения секрета, где k — пороговое число абонентов.

Разделение информации по схеме Шамира отличается размером частей секрета, определяемым разрядностью выбранного простого числа. Пусть размер секрета S определяется как $B_S = m+1$ бит, где $m = [\log_2 p]$, p — модуль схемы Шамира, $[\cdot]$ — оператор извлечения целой части числа. Секрет должен являться числом, меньшим основания p. Размер одного частного секрета $B_o^{\text{Ш}} = m+1 = B_S$. Полный объем памяти $B_{\text{П}}^{\text{Ш}} = nB_S$, где n — полное число абонентов.

Численный пример. Рассмотрим 3-из-5-схему Шамира и $B_S = 3$ Мбайт. Тогда $B_o^{\text{Ш}} = B_S = 3$ Мбайт и $B_{\text{П}}^{\text{Ш}} = 5B_S = 15$ Мбайт.

Определим затраты памяти на хранение остатков в соответствии с пороговой схемой на базе КТО [1.26] и размер секрета как $B_S = m+1$ бит. Пусть заданы большие взаимно простые числа $p_1 < p_2 < \ldots < p_{n-1} < p_n$, которые назовем основаниями пороговой криптосхемы. Секрет должен удовлетворять условию $\max(k-1) < S < \min(k)$, где $\min(k) = \prod_{i=1}^{k} p_i$, $\max(k-1) = \prod_{i=1}^{k-1} p_{n-k+1+i}$. Поэтому $m+1 \leqslant [\log_2 \Delta]$, где $\Delta = \min(k) - \max(k-1)$. Разрядности оснований для высокой криптостойкости пороговой схемы должны быть равными: $[\log_2 p_i] = d$, $i = 1, \ldots, n$. Следовательно, $[\log_2 \Delta] = kd + \sigma$, где σ — логарифмический дефект, k — пороговое число абонентов, и $m+1 \leqslant [\log_2 \Delta]$ [1.32]. Тогда размер одного частного секрета $B_o^{\text{КТО}} = \left\lceil \dfrac{m+1}{[\log_2 \Delta]} \right\rceil$ бит; объем памяти необходимый для хранения всех остаточных файлов $B_{\text{П}} = n \left\lceil \dfrac{m+1}{[\log_2 \Delta]} \right\rceil$ бит.

Численный пример. Пусть $B_S = 3$ Мбайт. Рассмотрим пороговую 3-из-5-схему, $d = 1$ Мбайт. Тогда $B_o = \dfrac{3}{3 \cdot 1} = 1$ Мбайт, $B_{\text{П}} = 5$ Мбайт, что значительно меньше затрат на хранение частей секрета по схеме Шамира.

Можно выделить два типа пролонгации: частей через смену ключа и частей без изменения секрета. Методы пролонгации модулярной пороговой схемы также базируются на смене частей, не затрагивая секрета [1.43, 1.44]. В основе данных методов лежит способ шифрования Эль-Гамаля.

ПС можно классифицировать по методу синхронизации работы пользователей в сети: синхронная и асинхронная пролонгированная система безопасности [1.42, 1.56]. Последний тип подразумевает асинхронный принцип взаимодействия абонентов: в асинхронной сети фазы смены ключа фиксируются дополнительно введенным синхронизатором, роль которого выполняет главный сервер. Современные компьютерные сети являются асинхронными, поэтому развитие методов асинхронной пролонгации ПС является необходимым.

Классифицируем методы пролонгации по взаимодействию с главным сервером.

1. Главный сервер формирует и передает секреты пользователям [1.45].

2. Абоненты обмениваются информацией с главным сервером, в результате чего формируется ключ [1.53].
3. Главный сервер отсутствует в пороговой схеме.

Наиболее интересными представляются методы, соответствующие третьему типу, поскольку они исключают атаку во время передачи секрета от сервера абонентам [1.30]. К данной группе можно отнести методы на основе обмена ключами Диффи–Хеллмана, метод формирования общего секрета на базе схемы Шамира [1.53], метод на основе эффекта синхронизации нейронных сетей [1.46, 1.52]. Главный недостаток данных методов — необходимость передачи данных по сети, что способствует проведению атаки активным противником посредством искажения передаваемой информации, что в свою очередь требует введения дополнительных методов верификации полученных данных. Другой подход заключается в построении пространственно разделенной между абонентами функции генерации секретов [1.55], которая позволяет получать каждому пользователю ПС свой секрет без обмена секретными данными по компьютерной сети.

В [1.18] для смены ключей предлагается использовать перебирающие последовательности, в частности последовательность элементов коммутативной группы поля Галуа, полученную посредством возведения в степень порождающего элемента, который является ключом криптосистемы. Данный метод предполагает наличие у каждого абонента генератора его частного секрета, который производит ключ после каждого сеанса и базируется на сложности задачи дискретного логарифмирования. Данный метод получил название «блуждающие ключи».

Разработка метода обновления секрета по принципу «блуждающих» ключей для модулярной пороговой схемы осложнена структурой доступа. Рассмотрим (k, n)-пороговую криптографическую схему пространственного разделения секрета на основе китайской теоремы об остатках (КТО), в которой n участников разделяют секретный ключ и только k или более из них могут восстановить секрет [1.26, 1.32]. Пусть заданы большие взаимно простые числа $p_1 < p_2 < \ldots < p_{n-1} < p_n$, которые назовем основаниями пороговой криптосистемы. Пусть $\min(k) = \prod_{i=1}^{k} p_i$, $\max(k-1) = \prod_{i=1}^{k-1} p_{n-k+1+i}$. Ключ S должен удовлетворять условию $\max(k-1) < S < \min(k)$. Так, для пороговой схемы (3, 4) должно выполняться условие $p_3 p_4 < S < p_1 p_2 p_3$, а для схемы (3, 5) — $p_4 p_5 < S < p_1 p_2 p_3$. Пороговое и полное числа абонентов связаны условием $n \geqslant k > 2$, где $[\cdot]$ — оператор извлечения целой части числа. Разность $\Delta = \min(k) - \max(k-1)$ должна быть достаточно большой: $\Delta \gg \max(k-1)$, для чего основания p_i должны быть близко расположены в числовом ряду; Δ определяет диапазон изменения ключа. Пусть $A = \{A_1, A_2, \ldots, A_n\}$ есть множество всех абонентов. Обозначим через V множество абонентов, которые решили восстановить секрет. Тогда (k, n) — пороговая структура доступа определится $D = \{V \subseteq A | |V| \geqslant k\}$. Множество подмножеств абонентов, которые не могут восстановить секрет, обозначим $N = \{V \subset A | |V| < k\}$. Пусть f есть псевдослучайная функция. Абоненты из A генерируют частные секреты посредством f при условии, что для всех S любая выборка абонентов $V \subseteq A$ может вычислить и восстановить $f(S)$, если $V \in D$, и не может восстановить $f(S)$, если $V \in N$. Если представить разделяемый секрет через его части $S = \{s_1, s_2, \ldots, s_n\}$, то основной задачей является нахождение представления $f(S) = \{f_1(s_1), f_2(s_2), \ldots, f_n(s_n)\}$. Выполнением преобразования f_i после каждого сеанса над остатками абонентов производится переход от одного ключа к другому. Важным условием для функции $f(S)$ является $\max(k-1) < f(S) < \min(k)$. Произведем выбор примитивных элементов полей $GF(p_1)$, $GF(p_2)$, $\ldots$, $GF(p_n)$ $g = (g_1, g_2, \ldots, g_n)$, таких что $g_i^2 > p_i$. Пусть $f(g) = (f_1(g_1), f_2(g_2), \ldots, f_n(g_n)) = (g_1^{v_1^j}, g_2^{v_2^j}, \ldots, g_n^{v_n^j})$, $v_i^j \in [1, p_i - 1]$,

$i = 1, 2, \ldots, n$. Генерация каждого последующего частного секрета производится последовательным увеличением степени $v_i^j = \left|v_i^{j-1} + \eta_i^j\right|_{p_i}$, где η_i^j — инкремент j-й фазы. При $\eta_i^j = 1$, $j = 1\,2\,\ldots$, выполнения условия $\max(k-1) < f(S) < \min(k)$ не происходит. Для данного случая необходимо произвести коррекцию результата возведения в степень, возвращая его в нужную область. Так, при $f(g) \leqslant \max(k-1)$ достаточно произвести сложение $f(g) + \max(k-1)$. Если $f(g) \geqslant \max(k-1)$, то область $\left[\min(k), \prod_{i=1}^{n} p_i\right)$ необходимо разбить на участки длиной Δ, число которых определится $l = \left[\dfrac{\prod_{i=1}^{n} p_i - \min(k)}{\Delta}\right]$, $\Delta' = \prod_{i=1}^{n} p_i - \min(k) - l\Delta$. Рисунок 1.8 поясняет данный подход.

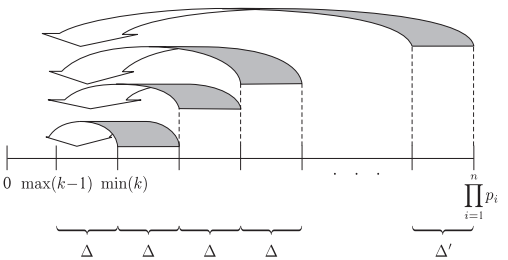


Рис. 1.8. Перевод чисел в разрешенную область пороговой схемы

Производить подобную проверку без объединения частей секрета абоненты не могут. Поэтому решением может выступать возведение в степень, взятую из определенного заранее списка, который хранит каждый абонент. Составление списка включает задачу дискретного логарифмирования: по числам из заданного диапазона и генератора элементов полей g_i определить соответствующие степени. При больших основаниях построение списка степеней займет много времени. Списки включают элементы соответствующих полей, число которых равно Δ в каждом. Если надежность системы защиты хранения списка от несанкционированного доступа достаточно высока, то нет причин хранить именно степени примитивного элемента, а не сами секреты.

Возведение в степень примитивного элемента поля Галуа может быть выполнено и над расширенным конечным полем. Возведение в степень полинома позволит формировать секрет из коэффициентов, разрядность которых равна разрядности характеристики поля $GF(p^n)$. Вычисления по модулю меньшей разрядности позволят сократить время на формирование ключа.

В теории ПС важным является вопрос верификации полученных пользователем частей секрета. Для ПС Шамира разработан [1.53, 1.54] метод проверки как в схеме с главным сервером, так и без него. Известные решения [1.19] для модулярной ПС основаны на введении дополнительной ПС Шамира и использовании метода из [1.53]. Данный подход представляется наименее приемлемым, поскольку увеличивает неоднородность криптографической системы, что ведет к снижению ее

криптостойкости [1.25]. Более перспективным является использование корректирующих возможностей СОК для обнаружения и локализации искаженных или ложных частных секретов. Известна работа по формированию групп для восстановления секрета по k частным секретам [1.50]. Разбиением производится управление процессом восстановления секрета, разграничение доступа к информации и исключается избыточная информация из данного процесса. Наличие избыточных оснований (число долей ключа больше k) в СОК позволяет проводить контроль и коррекцию ошибок. Следовательно, «подходящие» подгруппы в модулярной ПС должны содержать больше чем k абонентов.

Модулярная пороговая схема позволяет проводить пролонгацию посредством изменения полного и порогового числа пользователей, оснований и параметров генератора частных секретов [1.30, 1.51]. Пороговые схемы, в которых данные обновления выполняются без выхода системы безопасности из функционирующего состояния, называют динамическими ПС [1.41, 1.44, 1.47, 1.48, 1.49].

Проведение криптографических преобразований в полях Галуа [1.40] позволяет использовать вычислительные структуры из областей помехоустойчивого кодирования [1.23] и цифровой обработки сигналов [1.27, 1.28, 1.34] после соответствующей адаптации к задаче смены секрета по принципу «блуждающих» ключей. Формирование нового криптографического ключа является задачей повышенной размерности, что требует разработки специализированных вычислительных систем. Наиболее эффективным средством решения данной задачи являются нейроускорители, использующие возможности массовых параллельных вычислений [1.5, 1.36].

Отображение арифметики конечного поля на нейронную сеть в [1.37] основано на итеративном алгоритме понижения разрядности числа, представленного в позиционной системе счисления (ПСС):

$$A(j+1) = \sum_{i=0}^{\left[\log_b A(j)\right]} \left|b^i\right|_p \left\{A(j)\right\}^{[i]}, \qquad (1.2)$$

где b — основание ПСС; $\left\{A(j)\right\}^{[i]}$ — оператор извлечения i-го разряда b-ичного представления $A(j)$; $\left|b^i\right|_p$ — операция вычисления остатка целочисленного деления по модулю p. Вычислительная модель (1.2) реализует модулярную редукцию результатов операций сигнатуры поля $GF(p)$ и является моделью нейронной сети конечного кольца (НСКК) [1.36]. Рассмотрим обобщение принципа понижения разрядности результата операций на элементах конечного поля на случай его простого алгебраического расширения.

Пусть B — множество, образующее базис формирования элементов конечной алгебры. В $GF(p)$ элементами B выступают степени основания ПСС $\left(B_1 = \left\{b^i \mid i = 0, 1, 2, \ldots\right\}\right)$. В кольце многочленов от одной переменной $\Delta[x]$ выделяется два базиса, один из которых есть B_1, а второй есть множество степеней переменной x $\left(B_2 = \left\{x^i \mid i = 0, 1, 2, \ldots\right\}\right)$. Если в первом случае разрядность элемента определяется наибольшей степенью основания b в позиционном представлении числа, то во втором — наибольшей степенью элемента множества B_2.

Рекурсивная модель (1.2) определяет процесс разрядной редукции в простом поле $GF(p)$ через базис $\left|B_1\right|_p = \left\{\left|b^i\right|_p \mid i = 0, 1, 2, \ldots\right\}$. Расширение поля $GF(p)$ до $GF(p^n)$ за счет присоединения корня α неприводимого полинома $\pi(x)$ степени n приводит к расширению модели (1.2) включением вычетов по модулю $\pi(x)$ элементов базиса B_2: $\left|B_2\right|_{\pi(x)} = \left\{\left|x^i\right|_{\pi(x)} \mid i = 0, 1, 2, \ldots\right\}$. Тогда вычислительная модель

структурно-разрядной редукции произвольного многочлена степени s в элемент расширенного поля Галуа примет вид

$$P(x,\, j+1) = \sum_{k=0}^{s} \sum_{i=0}^{\left\lceil \log_b A(j) \right\rceil} \left| b^i \right|_p \left\{ A(j) \right\}^{[i]} \left| x^k \right|_{\pi(x)}. \tag{1.3}$$

Как и в [1.37] покажем, что операции $GF(p^n)$ основаны на модели (1.3):

$$P(x) \circ G(x) = F(x);$$
$$\left| F(x) \right|_{p,\pi(x)} = \left| P(x) \circ G(x) \right|_{p,\pi(x)} = \sum \left| f_v \right|_p \left| x^v \right|_{\pi(x)},$$

где $f_v = \sum_{\sigma+t=v} p_\sigma g_t$, если $\circ$ — операция умножения, или $f_v = p_v + g_v$, если $\circ$ — операция сложения.

Операции вычитания и деления в $GF(p^n)$ по модели (1.3) связаны с предварительным нахождением аддитивной и мультипликативной инверсий элемента соответственно, в данном конечном поле [1.20].

При сравнении моделей (1.2) и (1.3) можно выделить: процесс понижения разрядности на уровне базиса B_2 не является итеративным; рекурсия в (1.3) полностью определена моделью (1.2); если разрядность преобразованного по (1.2) числа равна или меньше разрядности основания p, то степень преобразованного полинома $\deg P(x,\, t)$ всегда меньше $\deg \pi(x)$.

Переход к вычислению секретного ключа над расширенным полем обусловлен сокращением разрядности операндов вычислителя за счет разбиения секрета на доли, число которых равно степени неприводимого полинома $\pi(x)$, разрядностью числа $(p-1)$. Секрет формируется посредством конкатенации коэффициентов редуцированного полинома. Эффект от данного перехода эквивалентен замене позиционной системы счисления на систему остаточных классов [1.7, 1.22]: распараллеливание вычислений на элементарном уровне, повышение живучести генератора секрета за счет многоканального представления.

Рассмотрим возможность генерации секрета в расширенных полях Галуа посредством возведения в степень порождающего элемента [1.33]. Обозначим через $D\big(m(x)\big)$ произвольную случайную функцию от порождающего полинома $m(x)$. Естественно, что данная функция содержит только мультипликативные операции. Примерами могут служить: степенная функция $\left| \big(m(x)\big)^v \right|_{\pi(x)}$, где v — случайная величина; произведение $\left| m(x) \cdot M(x) \right|_{\pi(x)}$, где $M(x)$ — случайный многочлен из поля $GF(p^n)$. Если имеет место разложение модуля на взаимно простые полиномы $p(x) = \prod_{i=1}^{l} \pi_i(x)$, где $\pi_i(x)$ — неразложимый многочлен над $GF(p)$, тогда согласно КТО [1.17] отображение $\Delta[x] \,/\, \big(p(x)\big) \to \prod_{i=1}^{l} \Delta[x] \,/\, \big(\pi_i(x)\big)$, где $\prod_{i=1}^{l}$ — прямое произведение, является изоморфным. Следовательно, возможна реализация модели (1.3) по l независимым каналам системы остаточных классов [1]. Известно [1.21, 1.38], что в случае факторизации модуля

$$p(x) = x^{p-1} - 1 = \prod_{k=1}^{p-1} (x + k) \tag{1.4}$$

при простом числе p произведение двух многочленов сводится к $p-1$ параллельным целочисленным умножениям в $GF(p)$ вместо $(p-1)^{1,59}$ методом Карацубы или $(p-1)\log(p-1)\log\log(p-1)$ методом Шенхаге–Штрассена. Обратимся к неприводимому полиному первой степени. Обозначим через g_i, $i=1, 2, \ldots m$, примитивные элементы поля $GF(p)$. Сформируем полином $P=(x+p-g_1)(x+p-g_2)\cdots(x+p-g_m)$, образующий конечное кольцо. Структура полинома позволяет:

- возведением в степень параллельно каждого g_i перебрать все элементы мультипликативной группы данного кольца;
- выбрав степень P через число примитивных элементов, обеспечить невыход ключа за определенный диапазон. Так, максимальная разрядность числа-секрета, получаемого конкатенацией коэффициентов элементов образованного кольца полиномов, определяется $z_{\max}=m([\log_2(p-1)]+1)$. В случае выбора всех примитивных элементов поля $GF(p)$ (т. е. при степени полинома P, равной m и $z=z_{\max}$) должно выполняться $[\log_2\Delta]=z_{\max}$, где Δ — правая граница диапазона изменения секрета;
- использовать простое число p относительно малой разрядности, что приводит к высокому быстродействию генератора секрета. Определим зависимость степени полинома $S(x)$ и разрядности p при известном Δ: $[\log_2(p-1)]+1=\dfrac{[\log_2\Delta]}{m}$. Для модулярной пороговой схемы $[\log_2\Delta]\approx k[\log_2(p_i-1)]$ при равенстве разрядностей оснований некоторому числу d получим $\left[\log_2(p-1)\right]+1=\dfrac{kd}{m}$. При $m>k$ выполняется данное свойство.

Параллельная реализация функции $D(m(x))$ по модулю (1.4) накладывает ограничения на характеристику p и размерность n поля $GF(p^n)$, а следовательно, на количество двоичных разрядов ключа

$$N=n([\log_2(p-1)]+1). \tag{1.5}$$

Максимальное количество параллельных вычислительных трактов равно $p-1$. На рис. 1.9 приведены соотношения (1.5) для 3-, 4-, 5-, 6- и 7-разрядных модулей. Поскольку поля $\Delta[x]\ /\ \big(p(x)\big)$ и $\Delta[x]\ /\ \big(\pi(x)\big)$ при $\deg p(x)=\deg\pi(x)=l$ содержат одинаковые элементы, то отображение $\prod\limits_{i=1}^{l}\Delta[x]\ /\ \big(\pi_i(x)\big)\xrightarrow{D(m(x))}\Delta[x]/\ /\ \big(\pi(x)\big)$ в $GF(p^n)$ определяет топологию нейросетевого генератора ключей.

Модуль p	$[\log_2(p-1)]+1$, бит	Разрядность ключа, бит	
		$n=\dfrac{p-1}{2}$	$n=p-1$
7	3	9	18
13	4	24	48
31	5	75	150
71	6	210	420
157	7	546	1092

Рис. 1.9. Зависимость разрядности секретного ключа от характеристики и степени поля Галуа порядка p^n

Рассмотрим предельный случай: $n = p - 1$. Восстановление результата $D(m(x))$ производится на основе КТО для системы (1.4):

$$D(m(x)) = \sum_{i=1}^{p-1} S_i(x) D_i(x) \bmod p(x),$$

где $D_u(x) \equiv D(m(x)) \pmod{x+u}$, $S_u(x) = T_u(x) \prod\limits_{\substack{i=1 \\ i \neq u}}^{p-1} (x+i)$, $T_u(x) \prod\limits_{\substack{i=1 \\ i \neq u}}^{p-1} (x+i) \equiv 1 \pmod{x+u}$. Так как $D_i(x)$ — целое число из $GF(p)$ и $\deg S_i(x) < \deg \pi(x)$, то $|D_i(x)|_{\pi(x)} = D_i(x)$ и $|S_i(x)|_{\pi(x)} = S_i(x)$, $i = 1, \ldots, p-1$. Поскольку $S_i(x) = \sum_{j=0}^{p-2} w_{ij} x^j$, $i = 1, \ldots, p-1$, то $D(m(x)) = \sum\limits_{j=0}^{p-2} \Big| \sum\limits_{i=1}^{p-1} |D_i(x)|_p w_{ij} \Big|_p x^j$. Следовательно, коэффициенты w_{ij}, $i = 1, \ldots, p-1$, $j = 0, \ldots, p-2$, образуют матрицу весовых коэффициентов нейронной сети

$$W = \begin{pmatrix} w_{10} & w_{20} & \ldots & w_{p-1\,0} \\ w_{11} & w_{21} & \ldots & w_{p-1\,1} \\ w_{12} & \ldots & \ldots & w_{p-1\,2} \\ \vdots & \ldots & \ldots & \vdots \\ w_{1\,p-2} & w_{2\,p-2} & \ldots & w_{p-1\,p-2} \end{pmatrix}.$$

Если $d = \begin{pmatrix} D_1(x) \\ D_2(x) \\ \vdots \\ D_{p-1}(x) \end{pmatrix}$, то $D(m(x)) = \big| W \cdot d \big|_p$.

На рис. 1.10 изображена структура описанной нейросетевой системы. Данная нейронная сеть содержит два слоя. Каждый слой включает $(p-1)$ НСКК. Первый слой предназначен для сокращения разрядности результатов случайной функции $\big|D_i(x)\big|_p$, $i = 1, \ldots, p-1$. Второй слой — для сокращения при восстановлении $D(m(x))$.

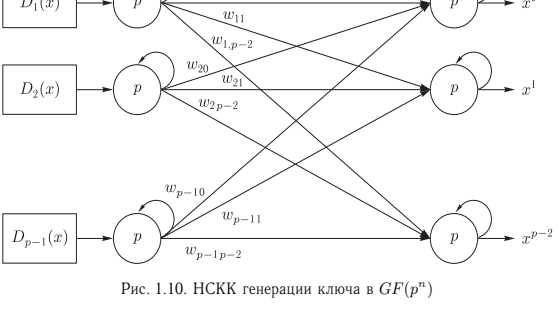


Рис. 1.10. НСКК генерации ключа в $GF(p^n)$