ФРАКТАЛЬНОЕ ШИФРОВАНИЕ

С. В. Кулешов

Санкт-Петербургский институт информатики и автоматизации РАН
199178, Санкт-Петербург, 14-я линия В.О., д. 39
kuleshov@mail.iias.spb.su

УДК 681.3.06
С. В. Кулешов. **Фрактальное шифрование** // Труды СПИИРАН. Вып. 2, т. 1. — СПб.: СПИИРАН, 2004.
Аннотация. *Предлагается подход к шифрованию, основанный на использовании фрактальных итерационных функций*. — Библ. 3 назв.

UDC 681.3.06
S. V. Kuleshov. **Fractal cipher** // SPIIRAS Proceedings. Issue 2, vol. 1. — SPb.: SPIIRAS, 2004.
Abstract. *The approach to the enciphering, based on use fractal iterative functions is offered.* — Bibl. 3 items.

В данной работе предлагается подход к нетрадиционному использованию фрактальных итерационных функций в шифровании передаваемых данных.

Предлагаемый итерационно-функциональный подход отличается от обычных методов шифрования тем, что фрактальная последовательность используется в качестве достаточно сложной кодирующей функции. При этом описание этой функции, достаточное для построения, является набором вещественных чисел, которые задают начальные условия итерационного процесса построения фрактальной последовательности. Предлагаемый подход является вариантом гаммирования — процесса "наложения" гамма-последовательности на открытые данные, где в качестве гамма-последовательности (последовательности псевдослучайных элементов) используется фрактальная последовательность.

Ключевой проблемой технических средств защиты информации является порождение действительно случайной последовательности битов. Дело в том, что генераторы случайных последовательностей, используемые для общих целей, являются псевдослучайными генераторами, так как в принципе существует конечное, а не бесконечное множество состояний ЭВМ. Более качественными генераторами случайных чисел являются генераторы, основанные на физических процессах (высокоточное измерение тепловых флуктуаций и др.)

Идея применения фрактальных сигналов как псевдослучайных последовательностей исходит из предположения возможности описания поведения физических и природных систем с помощью фракталов [1].

Фракталы относятся к множествам с крайне нерегулярной разветвленной или изрезанной структурой. Основные понятия теории фракталов, носящей междисциплинарный характер, пока еще находятся в процессе становления, но поле их приложения непрерывно расширяется. Большой интерес к фракталам связан с тем, что фракталы возникают в реальных задачах, причем в типичных, а не в экзотических ситуациях.

Теория фракталов рассматривает дробные меры вместо целочисленных и базируется на новых количественных показателях в виде дробных размерностей и соответствующих сигнатур. Фрактальные размерности характеризуют не только топологию объектов, но и отражают процессы эволюции динамических систем и связаны с их свойствами. Теория фракталов и нелинейность состав-

Труды СПИИРАН. 2004. Вып. 2. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2004. Issue 2. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

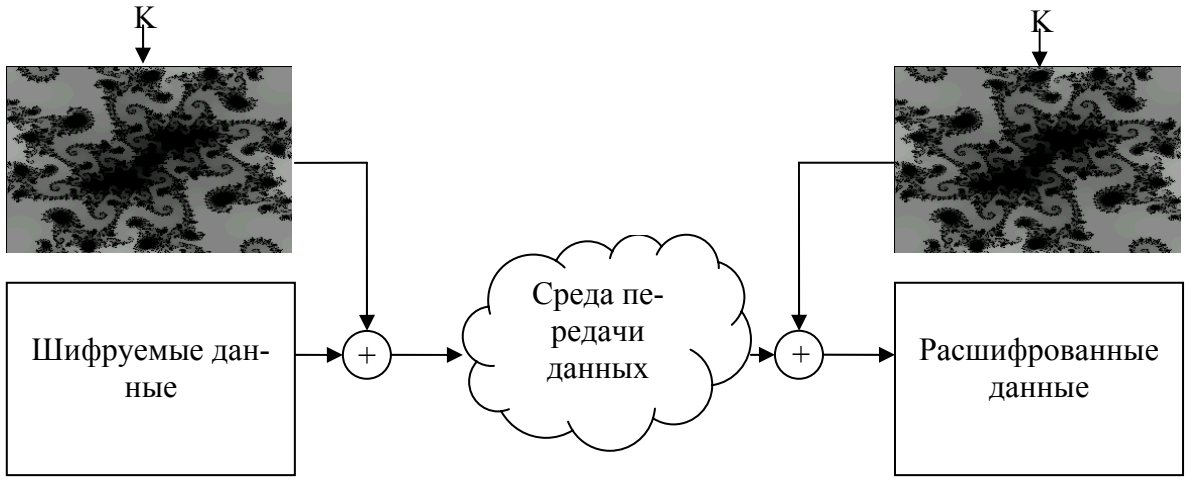
ляют геометрию хаоса. По своему содержанию контуры всех природных объектов суть динамические процессы, внезапно застывшие в физических формах, и объединяющие в себе устойчивость и хаос [2].

Применение шумоподобных систем, основанных на фрактальных сигналах, дает потенциальное преимущество над традиционными системами псевдослучайных последовательностей.

Исходная концепция выражается в развитии идеи «почему днем не видно звезд на небе», т.е. в искусственном добавлении к исходным данным шумоподобного сигнала. Чтобы «увидеть звезды» нужно «выключить» «закрывающее» их солнце. Наиболее наглядно принцип работы данного метода можно проиллюстрировать на одноцветных растровых изображениях.

Пусть исходное растровое изображение представлено яркостными отсчетами, расположенными в матрице прямоугольного вида. Построим по начальным условиям итерационный фрактал. Затем, применяя некоторую обратимую функцию (например, поразрядную сумму по модулю 2), к парам значений точек исходного изображения и изображения полученного фрактала, получим новое изображение, которое и передается по каналу связи. Для расшифровки сообщения требуется, зная начальные значения процедуры построения фрактальной последовательности, восстановить изображение фрактала и, применяя операцию, обратную по отношению к операции передающей стороны (в рассматриваемом примере это также сумма по модулю 2), восстановить исходное изображение.

Основная идея метода приведена на рис. 1. Как видно из схемы, сначала с помощью функции гаммирования вырабатывают гамма последовательность, которая зависит от параметра K, определяющего начальные значения итерационной функции. После этого исходный сигнал поразрядно суммируется с полученной гаммой по модулю 2.



РиРис.1. Идея фрактального шифрования

Для усложнения прямого подбора начальных значений фрактала последовательность позиций отсчетов (символов) исходного сигнала можно предварительно использовать перемешивание, применяя, например, заполняющую пространство кривую (ЗПК) [3]. При этом параметр начальной точки для ЗПК является дополнительным фактором, повышающим защищенность.

Начальные параметры итерационной функции, обеспечивающие выбор одного преобразования из совокупности возможных для данного алгоритма, являются криптографическим ключом.

Труды СПИИРАН. 2004. Вып. 2. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2004. Issue 2. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Важно подчеркнуть, что если начальные значения итерационной функции построения фрактала взяты вблизи точки аттрактора, то требуется очень точное представление данных чисел, так как в этом случае фрактал обладает качественной неоднозначностью, что усложняет задачу подбора значений. При этом итерационная функция, порождающая фрактальную последовательность, является вычислительно необратимой функцией, т.е. легко вычислима в прямом направлении, в то время как определение значения ее аргумента при известном значении самой функции обладает сложностью, эквивалентной полному перебору. Иными словами, вычисление обратного преобразования не может быть произведено более эффективным способом, чем перебором по множеству возможных значений начальных параметров функции. Так как итерационный процесс построения фрактала относительно долгий процесс, что при процедуре полного перебора начальных значений с последующим восстановлением фрактала и последующим расшифрованием требует больших вычислительно-временных ресурсов.

Задача фрактального шифрования позволяет переформулировать задачу криптографии в терминах сложности по А. Н. Колмогорову [4] как построение минимальной программы, порождающей псевдослучайную последовательность, при известных параметрах ключа и невозможность построения короткой программы восстановления последовательности при неизвестном ключе. При этом сложность данных, согласно Колмогорову, определяется как минимально возможная длина программы для машины Тьюринга, которая может сгенерировать рассматриваемый набор данных.

Численный эксперимент, проведенный на параллельном вычислительном кластере, показал отсутствие различных наборов начальных значений приводящих к построению одинаковой гамма-последовательности, используемой для шифрования. Это позволяет утверждать значимость всех битов ключа, а следовательно и длину (по Колмогорову) дешифрирующей программы.

Кроме того, рассматриваемый метод осуществляет описание дискретного множества, в отличие от функционального описания бесконечного множество точек. При этом фрактал является механизмом построения множества, которое удовлетворяет требованиям псевдослучайной последовательности.

Аутентичность передаваемых данных может быть установлена традиционными методами подсчета контрольной суммы или другими методами.

Настоящий метод применим для любых типов данных. При этом шифруемая последовательность кодов символов (текст) или отсчетов некоторой физической величины (звук) располагается по строкам прямоугольной матрицы, после чего применяют описанный выше метод.

Фрактального шифрование также демонстрирует возможность передачи дополнительной информации без увеличения объема передаваемых данных.

Численный эксперимент, производящий полный перебор с постоянным шагом по начальным значениям итерационной функции, показал тенденцию быстрого уменьшения значения минимальной ошибки на интервале при приближении к начальным значениям заданных параметров итерационной функции при переборе с большим шагом, в то время, как с уменьшением шага перебора начинают проявляться хаотические свойства фрактального сигнала, что не позволяет осуществлять поиск начальных параметров более эффективным способом, чем полный перебор.

Форма зависимости, полученная экспериментально, приведена на рис. 2. Верхний график показывает изменение ошибки (ось ординат) при переборе по

Труды СПИИРАН. 2004. Вып. 2. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2004. Issue 2. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

всей области значений (ось абсцисс) начальных параметров. Выделенный фрагмент в увеличенном масштабе показан на нижнем графике. Истинное значение начального параметра показано пунктирной линией.

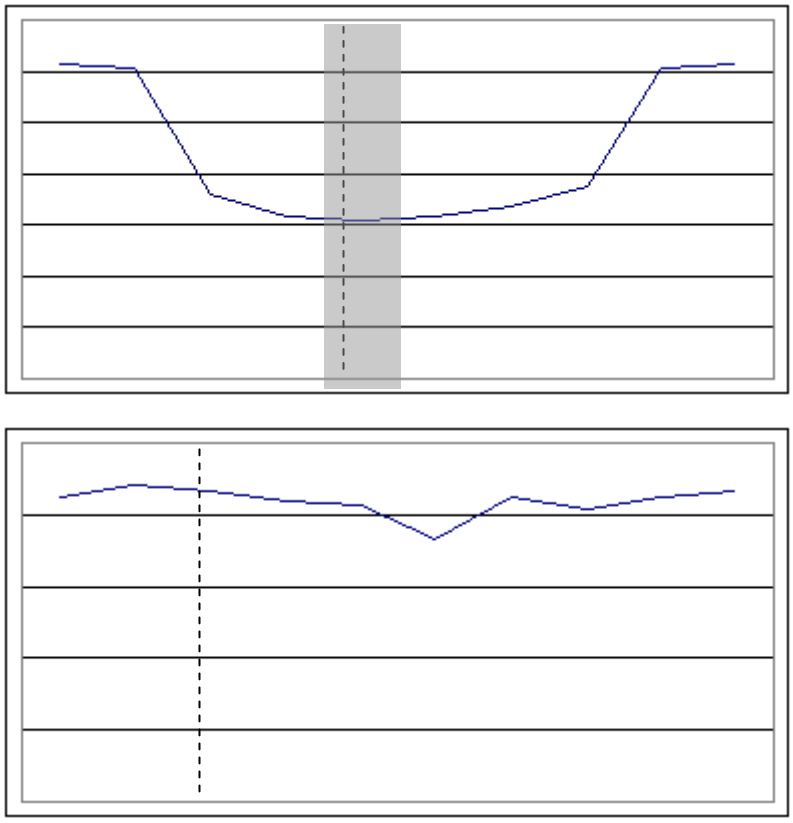


Рис. 2. Зависимость значения минимальной ошибки от выбора начального параметра итерационной функции

Отличительным свойством фрактального шифрования является проявление хаотических свойств фрактального сигнала (аналог большой длины криптографического ключа) только при использовании начальных значений, определенных с высокой точностью, что требует предварительного составления каталога функций, удовлетворяющих заданным свойствам для эффективного выбора ключа для шифрования. При этом форма зависимости определяется видом конкретного итерационного функционала из каталога.

Так как фракталы обладают свойством симметрии, то при применении фрактального сигнала требуется учитывать эти особенности и использовать в качестве гаммы асимметричные фрагменты, так как симметрия фрактальных сигналов также позволяет сократить область перебора при дешифровании.

Криптографическая стойкость полученного алгоритма, а также оптимальные виды фракталов, дающие минимальный размер ключа при максимальной устойчивости шифросистемы представляет предмет дальнейших исследований.

При оптимальном выборе начальных условий итерационного процесса и использовании асимметричного фрагмента фрактала можно обеспечить значимость всех битов выбранного ключа при выполнении операции шифрования. Полученный сигнал сложно отличить от шума, к тому же для расшифровки необходимо знать конкретный вид динамической системы и начальный параметр процесса.

Труды СПИИРАН. 2004. Вып. 2. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2004. Issue 2. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Таким образом, использование фрактального подхода в шифровании может дать мощный и эффективный механизм формирования функции гаммы, имеющую сильную зависимость от параметров ключа.

Приведенный пример фрактального шифрования раскрывает иной концептуальный подход у организации процедуры, как сокрытия, так и возможного дополнительного внедрения информационного содержания.

Литература

[1] *Александров В. В.* Развивающиеся системы. В науке, технике, обществе и культуре: Учебное пособие. СПб.: Изд-во СПбГТУ, 2000. 243 с.

[2] *Гуляев Ю. В. и др.* Математика и физика фракталов: теоремы, модели, некоторые результаты // Тезисы докладов XLVI конференции МФТИ. 2003. С. 58-59.

[3] *Александров В. В., Арсентьева А. В.* Информация и развивающиеся структуры. Л.: ЛИИАН, 1984. 182 с.

[4] *Колмогоров А. Н.* Три подхода к количественному определению информации // Проблемы передачи информации. 1965. Т. 1, вып. 1. С. 124-126.