КРИПТОЗАЩИТА ДАННЫХ НА ОСНОВЕ СИСТЕМ ФАЗОВОЙ СИНХРОНИЗАЦИИ

Бывшев С. С.
Кафедра теоретических основ электротехники
Научный руководитель: Шилин Л.Ю., декан ФИТиУ, д - р техн. наук, проф.

Аннотация **– Изложен принцип моделирования генератора случайной последовательности, использующего особенности работы системы фазовой синхронизации в хаотическом режиме. Описываетсяся возможная программная реализация криптосистемы шифрования данных на основе смоделированного генератора.**

[5] ***Ключевые слова: иммитационное моделирование; режим хаоса; генератор случайных чисел; поточная криптоситема.***

Рассматриваются системы ФАПЧ (фазовой автоподстройки частоты), являющиеся разновидностью систем фазовой синхронизации, которые широко используются для стабилизации и синтеза частоты.

Для подобных систем характерны различные режимы работы: установившийся режим, неустановившийся режим, режимы хаоса. С точки зрения практического применения, наиболее интересен режим детерминированного хаоса. Этот вид режима работы обусловлен наличием нелинейности в системе. Режим является нерегулярным. Причина нерегулярности определяется свойством нелинейных систем экспоненциально быстро разводить первоначально близкие траектории.[1] Поэтому не представляется возможным предсказать поведение таких систем, так как реально начальные условия можно задавать лишь с конечной точностью, а ошибки экспоненциально возрастают. Данный режим характеризуется построением странных аттракторов в области фазового пространства (Рисунок 1).

Ранее была разработана имитационная модель системы ФАПЧ, которая обладает достаточной гибкостью, с целью использования её составных блоков в других приложениях. В частности, алгоритм работы фазового дискриминатора в режиме детерминированного хаоса предлагается использовать для генерации гамма-ключа, применяемого при обратимом кодировании файлов. В качестве случайных последовательностей будут использоваться значения фазы и частоты сигнала на выходе блока фильтров модели.

Предлагается на основе иммитационной модели создать систему щифрования информации для передачи последней по открытым каналам связи. Будем использовать симметричный алгоритм шифрования, в котором шифрование и дешифрование отличается только порядком выполнения и направлением некоторых шагов. В этом алгоритме будет использоваться один и тот же секретный ключ – физические параметры работы модели. С точки зрения простоты реализации, наиболее привлекательным является двоичное (битовое) гаммирование. Этот способ предполагает, что шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Т.е. осуществляется побитовое сложение n-битового открытого текста и n-битового ключа. Обычно, при использовании гаммирования, если гамма короче, чем открытое сообщение, она повторяется требуемое число раз. В нашем случае, в этом нет необходимости, так как возможно сгенерировать гамма последовательность необходимой длины. Этот аспект позволяет построить поточную систему шифрования данных, которая сможет передавать поток данных, каждый символ которых должен быть зашифрован и отправлен куда-либо, не дожидаясь последующих данных (обмен текстовыми и голосовыми сообщениями по сети).

При кодировании файла целиком (без учета структуры), снижается криптостойкость шифра. Это объясняется тем, что многие файлы помимо основных данных, хранят однородные данные о формате. Поэтому для некоторых форматов файлов целесообразно шифровать только основные данные. Например, при шифровании текстовых файлов будем преобразовывать символы в коды таблицы соответствующей кодировки (например, ANSI, UNICODE). Далее производить преобразование над кольцом, мощность которого соответствует размеру таблицы кодировки. Для повышения криптостойкости можно провести обратное отображение кодов в символы. При шифровании изображений таким способом необходимо получить каждый пиксель изображении. Затем получить значения каналов RGB(Red, Green, Blue) и выполнить гаммирование каждого канала.

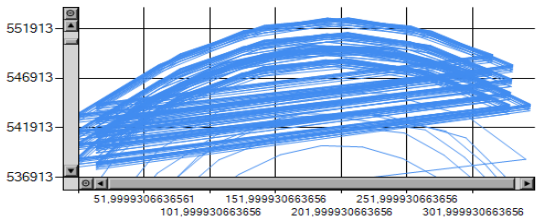

Рис. 1. Фазовый портрет системы в режиме детерминированного хаоса

Таким образом, разработанная криптосистема обладает рядом неоспоримых преимуществ: достаточно большая мощность ключевого пространства и гаммы, высокая скорость шифрования, простая алгоритмическая организация.

[1] Акимов В.Н., Белюстина Л.Н., Белых В.Н. Системы фазовой синхронизации // М.: Радио и связь, 1982. -288 с.

[2] Еремеев Г.В., Кузнецов А.П., Шилин Л.Ю. Моделирование систем импульсно-фазовой АПЧ, работающей на кратных частотах // Изв. Вузов. Приборостроение: 1990. -98 с.

[3] Шахгильдян В.В., Ляховкин А.А. Системы фазовой автоподстройки частоты // М.: Связь, 1972. -447 с..