ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ НА ОСНОВЕ ХАОТИЧЕСКОЙ ДИНАМИКИ МАГНИТНОГО МАЯТНИКА

Кудан Т.А., Манько А.А. студенты

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Андрианова Е.В. – ассистент

Аннотация. Предложен метод генерации криптографических ключей на базе нелинейной динамики магнитного маятника. Разработана математическая модель его движения в поле трех притягивающих центров с учетом высоты подвеса и квазиупругой силы. Описан алгоритм интегрирования уравнений движения симплектическим методом Бимана. Обоснована методика преобразования флуктуаций начальных условий в равномерно распределенный битовый массив через криптографическое хеширование. Предложен метод построения криптографически стойкого генератора псевдослучайных чисел (ГПСЧ) с открытым исходным кодом (open-source), стойкость которого основана на свойствах детерминированного хаоса.

Введение. Фундаментальной задачей криптографии и статистического моделирования является получение качественных случайных последовательностей. Стандартные алгоритмические генераторы псевдослучайных чисел (ГПСЧ) уязвимы при компрометации их начального состояния (seed), так как работают по детерминированным математическим правилам. Для обеспечения высокого уровня безопасности применяются аппаратные генераторы истинно случайных чисел (ГИСЧ), использующие физические процессы, например, квантовые флуктуации или тепловой шум, к которым предъявляются строгие стандарты оценки энтропии [6].

В современных процессорах (Intel, AMD) существуют встроенные аппаратные инструкции (например, RDRAND), генерирующие случайные числа на основе теплового шума транзисторов с высокой скоростью [5]. Однако использование таких решений в критически важных системах сопряжено с проблемой доверия. Архитектура промышленных процессоров закрыта (принцип «черного ящика»), что делает невозможным независимый аудит схемы на предмет наличия аппаратных закладок или бэкдоров, теоретически позволяющих спецслужбам или производителю предсказывать выходные значения.

В данной работе предлагается концепция «прозрачного» ГПСЧ. В качестве основы алгоритма используется математическая модель макроскопической динамической системы — магнитного маятника. В отличие от стандартных математических абстракций, логика работы данного генератора полностью прозрачна и опирается на физическую теорию динамического хаоса. Система демонстрирует режим детерминированного хаоса: обладая строгим математическим описанием [2], она характеризуется экспоненциальной неустойчивостью фазовых траекторий (положительностью максимального показателя Ляпунова), что делает долгосрочное предсказание ее поведения невозможным при наличии малейших погрешностей измерения начальных условий.

Основная часть. В качестве концептуальной модели системы рассматривается сферический маятник, совершающий колебания в гравитационном поле над горизонтальной плоскостью, на которой закреплены три постоянных магнита. Геометрическая схема установки и выбранная декартова система координат представлены на рисунке 1. Груз маятника снабжен магнитом, ориентированным на притяжение к магнитам в основании.

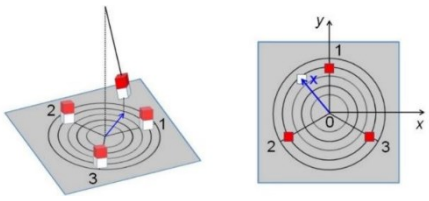

Рисунок 1 – Схема расположения магнитов и системы координат модели

Движение описывается в двумерном приближении малых колебаний радиус-вектором положения в плоскости xy: $\vec{r} = (x, y)$. Согласно второму закону Ньютона, вектор ускорения $\vec{a} = \vec{r}$ определяется суперпозицией действующих сил, отнесенных к массе маятника. В разработанной модели учитываются три ключевых взаимодействия:

1 Квазиупругая возвращающая сила: в приближении малых углов отклонения проекция гравитационной силы на плоскость xy, стремящаяся вернуть маятник в положение равновесия, пропорциональна смещению. В кинематической модели она характеризуется квадратом круговой (собственной) частоты малых колебаний $\omega_0^2 = \frac{g}{L}$ (где g — ускорение свободного падения, L — эффективная длина подвеса).

2. Сила вязкого трения: сопротивление среды, пропорциональное вектору скорости движения $\vec{v} = \dot{\vec{r}}$, характеризуется удельным коэффициентом затухания μ.

3. Магнитное взаимодействие: сила притяжения к каждому из магнитов рассчитывается с учетом постоянного расстояния h по вертикали от плоскости движения груза до плоскости магнитов. Введение параметра h необходимо для корректного моделирования проекции трехмерного поля диполя на двумерную плоскость движения и предотвращения сингулярностей (деления на ноль при прохождении точно над магнитом).

Итоговое дифференциальное уравнение движения (для ускорения) имеет вид (1):

$$\vec{a} = -\mu\vec{v} - \omega_0^2\vec{r} + \sum_{m=1}^{3} \frac{\overrightarrow{r_m}}{\left(h^2 + |\overrightarrow{r_m}|^2\right)^{\frac{3}{2}}}, \quad (1)$$

где $\overrightarrow{r_m}$ – вектор, направленный от маятника к m-му магниту, а знаменатель в формуле (1) $(h^2 + |\overrightarrow{r_m}|^2)^{\frac{3}{2}}$ соответствует закону убывания силы для магнитного диполя с учетом вертикального смещения.

Программная реализация выполнена на C#. Для интегрирования уравнений применен алгоритм Бимана [4], обеспечивающий устойчивое численное интегрирование уравнений движения.

Компьютерная модель трансформирует физическую энтропию в цифровой ключ. Источником первичного уникального зерна (seed) служат младшие разряды системного таймера высокой точности и текущее состояние ОЗУ. Программный модуль симулирует движение маятника до диссипации энергии (полной остановки). Фиксируются два параметра конечного состояния: индекс магнита-аттрактора и длительность переходного процесса. Поскольку одна итерация дает мало энтропии, система проводит серию симуляций с микроскопическим возмущением начальных условий [3]. Полученный массив данных конкатенируется и сжимается криптографической хеш-функцией SHA-256 [7] до равномерно распределенной последовательности длиной 256 бит.

Моделирование для сетки из 800×800 начальных состояний (всего 640 000 индивидуальных траекторий до остановки) позволило получить карту бассейнов притяжения системы (Рисунок 2). Визуализация подтверждает наличие развитой фрактальной структуры границ между областями притяжения магнитов. Это свидетельствует о том, что даже микроскопические изменения начальных условий (на уровне 10^{-6}) приводят к изменению конечного состояния макросистемы, обеспечивая высокую криптографическую стойкость генератора. Основным ограничением является низкая производительность (~15–50 кбит/с), обусловленная вычислительной сложностью метода Бимана, что позиционирует комплекс как решение для генерации мастер-ключей, а не потоковых задач.

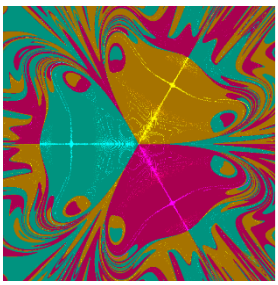

Рисунок 2 – Визуализация фрактальных границ областей притяжения)

Список использованных источников

1.Анищенко, В. С. Сложные колебания в простых системах: механизмы возникновения, структура и свойства динамического хаоса / В. С. Анищенко. – Москва : Наука, 1990. – 312 с.

2.Кузнецов, С. П. Динамический хаос: курс лекций / С. П. Кузнецов. – Москва : Физматлит, 2001. – 296 с.

3.Alvarez, G. Some basic cryptographic requirements for chaos-based cryptosystems / G. Alvarez, S. Li // International Journal of Bifurcation and Chaos. – 2006. – Vol. 16, iss. 8. – P. 2129–2151.

4.Beeman, D. Some multistep methods for use in molecular dynamics calculations / D. Beeman // Journal of Computational Physics. – 1976. – Vol. 20, iss. 2. – P. 130–139.

5.Intel Digital Random Number Generator (DRNG) Software Implementation Guide [Electronic resource] / Intel Corporation. – 2018. – Mode of access: https://www.intel.com/content/www/us/en/developer/articles/guide/intel-digital-random-number-generator-drng-software-implementationguide.html. – Date of access: 06.03.2026.

6.Recommendation for the Entropy Sources Used for Random Bit Generation : NIST SP 800-90B [Electronic resource] / National Institute of Standards and Technology. – Gaithersburg : NIST, 2018. – Mode of access: https://csrc.nist.gov/publications/detail/sp/800-90b/final. – Date of access: 06.03.2026.

7.Secure Hash Standard (SHS) : FIPS PUB 180-4 [Electronic resource] / National Institute of Standards and Technology. – Gaithersburg : NIST, 2015. – Mode of access: https://csrc.nist.gov/publications/detail/fips/180/4/final. – Date of access: 06.03.2026.