УДК 004.056

К.В. АГИЕВЕЦ[2], М.А. ИВАНОВ[1,2]

[1]Государственный университет управления, Москва
[2]Национальный исследовательский ядерный университет «МИФИ», Москва

ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ПРЕДНАЗНАЧЕННЫЙ ДЛЯ СОЗДАНИЯ ВИРТУАЛЬНОГО КАНАЛА СВЯЗИ В СХЕМЕ СТОХАСТИЧЕСКОГО КОДИРОВАНИЯ

Рассматривается устройство, ориентированное на реализацию прямого и обратного стохастического преобразования в стохастическом (n, k, Q) кодеке. Блок прямого стохастического преобразования, реальный дискретный канал связи и блок обратного стохастического преобразования образуют Q-ичный симметричный канал, в котором в случае ошибки в канале связи вероятности различных векторов ошибок Q-ичных символов равны.

При передаче данных по каналам связи приходится решать три задачи защиты информации: обнаружение и исправление ошибок, вызванных действием помех в каналах связи (обеспечение помехозащищенности); обеспечение секретности информации; защиту от навязывания ложных данных (имитозащиту).

Известен способ обеспечения комплексной защиты информации, пересылаемой по каналу связи, основанный на использовании стохастического кодирования [1, 2]. В докладе рассматривается генератор псевдослучайных чисел (ГПСЧ), ориентированный на реализацию прямого и обратного стохастического преобразования в стохастическом (n, k, Q) кодеке, где n – число Q-ичных символов в кодовом слове, k – число информационных Q-ичных символов, (n – k) – число проверочных Q-ичных символов.

На рис. 1 показана схема ГПСЧ, где DI – информационные входы, Mode – вход режима, Clk – тактовый вход, K – ключ (параметр стохастического преобразования); Rg – регистры, Mux – мультиплексоры (два в один), блок сложения в $GF(2^{L/2})$, блок умножения на матрицу $(T_G)^{L/2}$ (T_G – матрица размером $L/2 \times L/2$, определяющая один такт работы генератора Галуа, вид которой зависит от выбранного характеристического двоичного примитивного многочлена $L/2$-й степени), блок замены S, блок сложения по модулю $2^{L/2}$; DO – информационные

выходы устройства в режиме стохастического преобразования, L – разрядность Q-ичных символов.

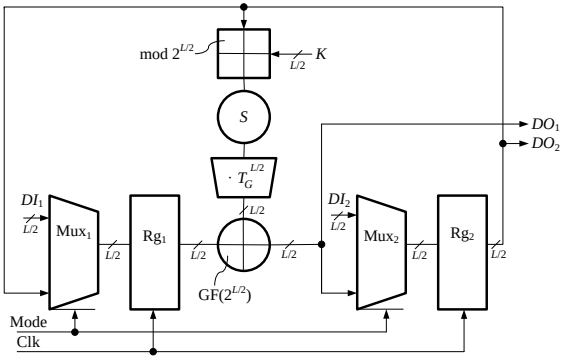

Рис. Схема ГПСЧ

В устройстве реализована сеть Фейстеля, обладающая свойством обратимости выполняемых криптографических преобразований, что дает возможность по одной и той же схеме реализовать прямое (на стороне источника информации) и обратное стохастическое преобразование (на стороне приемника информации), что является необходимым условием при реализации стохастического кодирования информации. При этом раундовая функция петли Фейстеля может быть реализована на основе 2D или 3D (в зависимости от величины L) S-блока и блока умножения на матрицу.

При $L = 32$ выбирается 2D S-блок размером 4×4; при $L = 128$ выбирается либо 2D S-блок размером 8×8, либо 3D S-блок размером $4 \times 4 \times 4$.

Список литературы

1. Алгоритмическое мышление в задаче надежной передачи данных по каналу связи. Агиевец К.В., Иванов М.А., Кондахчан М.А., Стариковский А.В. − Вторая Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность» (КИБ-2024). Сборник научных трудов. – М.: НИЯУ МИФИ, 2024. – С. 92–93.

2. Ватрухин Е.М. Комплексная защита информации в каналах «земля-борт» // Вестник Концерна ВКО «Алмаз-Антей». 2020, № 4. – С. 6–14. https://doi.org/10.38013/2542-0542-2020-4-6-14