ПРИМЕНЕНИЕ РАСШИРЕННЫХ ПОЛЕЙ ГАЛУА $GF(2^v)$ ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ СКРЫТНОСТИ ПЕРЕДАЧИ ДАННЫХ

Калмыков И.А., Чипига А.А., Хайватов А.Б., Сагдеев А.К.

Ставропольский военный институт связи Ракетных войск,

Северо-Кавказский государственный технический университет,
г. Ставрополь, Россия

kia762@yandex.ru

Проблема исследований: В настоящее время наблюдается тенденция сращивания систем военного и государственного назначения с коммерческими и широкодоступными компьютерными системами и сетями. При этом возникают новые задачи по обеспечению безопасности информации в незащищенной среде от возрастающих угроз, направленных на раскрытие содержания информации и нарушение ее целостности.

Решение проблемы: В последние годы наблюдается тенденция все более всестороннего применения алгебраических систем конечных полей Галуа при построении адаптивных средств защиты информации.

Известно, что при реализации поточного и блочного шифрования в симметричных криптографических системах широкое применение нашли двоичные псевдослучайные последовательности (ПСП). Обладая хорошими статистическими характеристиками, данные ПСП характеризуются следующими недостатками:

- структура генератора ПСП будет известна при обработке $2n$ символов ПСП, где n – разрядность генератора;

- ПСП, снимаемые с различных элементов памяти являются циклически сдвинутыми друг относительно друга.

Основные пути повышения эффективности генераторов ПСП:

- модификация генераторов ПСП;

- использование алгебраических систем полей Галуа $GF(2^v)$.

При использовании М-последовательности она снимается с одного элемента задержки генератора, и в каждый момент времени может быть зашифро-

ван только один бит информации открытого текста. Тогда операция суммирования по модулю два является единственной обратимой функцией шифрования.

Для использования алгебраической системы расширенных полей Галуа при обеспечении информационной скрытности передачи данных необходимо иметь не двоичную последовательность, а элементы соответствующего поля $GF(2^v)$. Тогда информация должна сниматься параллельным кодом с v ячеек регистра сдвига. Порядок считывания информации с выбранных линий задержки регистра сдвига может быть выбран любой.

Так как в результате будут получены элементы расширенного поля Галуа $GF(2^v)$, порождаемые характеристическим многочленом (**порождающим полиномом**) $g(z)$, которые составляют мультипликативную и аддитивную группу, то к ним могут быть применены разнообразные функции:

- сложение элементов по модулю порождающего полинома $g(z)$;
- умножение элементов поля по модулю порождающего полинома $g(z)$;
- возведение элементов в степень по модулю $g(z)$.

С одного регистра сдвига ПСП могут сниматься несколько последовательностей элементов расширенного поля Галуа $\{g_1(z), g_2(z)...\}$. Тогда существует возможность использования линейных и нелинейных преобразований:

$$s(z)g_1(z) + g_2(z) \equiv f(z) \bmod g(z), \quad (1)$$

$$s(z)^{g_1(z)} g_2(z) + g_3(z) \equiv f(z) \bmod g(z), \quad (2)$$

$$s(z)^{g_1(z)} + g_2(z)^{g_3(z)} \equiv f(z) \bmod g(z), \quad (3)$$

где $s(z)$ – элемент открытого текста; $f(z)$ – элемент зашифрованного текста.

Для реализации операции кодирования информации на передающей стороне осуществляется деление исходного сигнала на блоки длиной $s(z) = ordg(z)$, получение ПСП элементов расширенного поля Галуа $\{g_1(z), g_2(z)...\}$, а также выполнение линейных и нелинейных преобразований (1)-(3), включающих операции сложения, умножения и возведение в степень элементов в поле $GF(2^v)$. Поскольку для обеспечения информационной скрытности используются две и более ПСП элементов поля $GF(2^v)$, то при этом обеспечивается высокая стойкость к атакам, а вскрытие состояния регистра сдвига

может быть обеспечено только путем тотального перебора всего множества состояний.

Литература

1. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов/ Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2005. - 276 с.

2. Элементы применения компьютерной математики и нейроинформатики /Н.И. Червяков, И.А. Калмыков И.А., В.А. Галкина, Ю.О. Щелкунова, А.А. Шилов; Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2003. – 216с.