ответствии с алгоритмом работы обнаружителя, представленного в [6], определяется наличие или отсутствие сигнала на входе приемника. При наличии сигнала САПД запоминает полученные значения $D_{\varsigma+i}$ и $A_{\varsigma+i}$ и продолжает набор статистических данных, соответствующих с требуемым значениям погрешности определения мощности шума и точности синхронизации. После этого в соответствии с решающим правилом (8) и алгоритмом оценивания мощности шума, представленным в [5], определяется значение временного сдвига сетки тактовых импульсов передатчика и приемника, и искомое значение мощности шума в канале связи. Сведения о наличии сигнала, мощности шума и о временном рассогласовании передатчика и приемника поступают на вход устройства выдачи исходных данных (УВИД), которое в соответствии с логикой работы демодулятора выдает требуемую информацию.

### Литература


1. Николаев Б.И. Последовательная передача дискретных сообщений по непрерывным каналам с памятью. М.: Радио и связь, 1988. – 262 с.
2. Финк Л.М. Теория передачи дискретных сообщений. М.: Сов. радио, 1970. – 728 с.
3. Кузнецов А.И., Халилов Р.Р. Тактовая синхронизация в каналах с межсимвольной интерференцией на основе структурного анализа многолучевого сигнала // ИКТ. Т.4, №1, 2007. – С. 41-43.
4. Котлова Т.В., Халилов Р.Р. Оценка порогового уровня различения «ненулевых» фрагментов сигнала для алгоритма тактовой синхронизации, основанного на повторяемости частей принимаемого многолучевого сигнала // Сб. докладов ВНТК «Актуальные проблемы ракетно-космической техники и ее роль в устойчивом социально-экономическом развитии общества». Самара, 2009. – С. 209-210.
5. Халилов Р.Р. Оценивание дисперсии шума в каналах с МСИ с использованием метода дифференциального анализа. // Сб. докладов IX МНТК Проблемы техники и технологий телекоммуникаций. Казань, 2008. – С. 219-220.
6. Халилов Р.Р. Обнаружение сигналов в каналах с межсимвольной интерференцией и шумом. // Сб. докладов V НТК Системы наблюдения, мониторинга и дистанционного зондирования Земли. Москва, 2008. – С. 76 – 80.
7. Кловский Д.Д., Сойфер В.А. Обработка пространственно-временных сигналов. М.: Связь, 1976. – 208 с.


## SIGNAL DETERMINATION PROCEDURE, ESTIMATION OF NOISE DISPERTION AND BIT TIMING VIA MULTIPATH CHANNELS

**Kotlova T.V., Khalilov R.R.**

**This article represents bit timing algorithm, statistic simulation of suggested algorithm, operation scheme of joint signal detecting device, as well as estimation of channel noise dispersion and bit timing which is based on segment repetition of sensed multipath signal.**

***Keywords:*** *signal, detection, bit timing, noise dispersion, simulation, multi-path.*

Котлова Татьяна Викторовна, инженер-программист 2 категории ГНПРКЦ «ЦСКБ-Прогресс». Тел. 8-902-336-59-43, E-mail: tatiana.kotlova@gmail.com

Халилов Ринат Рашидович, заместитель начальника Центра получения и обработки информации «Самара» ГНПРКЦ «ЦСКБ-Прогресс». Тел. 8-903-308-21-68, E-mail: halilovr82@mail.ru

УДК 681.3

# ТЕХНОЛОГИЯ НЕЛИНЕЙНОГО ШИФРОВАНИЯ ДАННЫХ В ВЫСОКОСКОРОСТНЫХ СЕТЯХ СВЯЗИ

*Калмыков И.А., Стрекалов Ю.А., Щелкунова Ю.О., Кихтенко О.А., Барильская А.В.*

В статье рассмотрена технология построения криптосистемы нелинейного шифрования данных с использованием полиномиальной системы классов вычетов. Предложен метод, позволяющий обеспечить высокую скорость шифрования потока данных.

***Ключевые слова:*** нетрадиционные алгоритмы шифрования, поля Галуа, полиномиальная система классов вычетов, нелинейное шифрование данных.

### Введение

Широкое использование информационных систем в государственных учреждениях, финансовых структурах и военно-промышленном комплексе, а также быстрое развитие информационных систем общего пользования вызвало необходимость разработки средств защиты от несанкционированного

доступа к информации и аутентификации пользователей [1-8]. Одним из критериев жизнеспособности современного государства является наличие защищенного, динамически развивающегося информационного пространства, пронизывающего все среды деятельности государства. На практике такое пространство складывается из информационных и автоматизированных систем управления, объединенных коммуникациями, и их создание становится задачей первостепенной важности.

Применение вычислительной техники в различных областях предопределяет необходимость разработки и создания адаптивных средств защиты информации в вычислительных сетях от несанкционированного доступа (НСД).

## Основная часть

Защита информации представляет собой комплекс мероприятий, направленных на предотвращение несанкционированной утечки, модификации и удаления информации, осуществляемых с применением технических, в том числе и программных, средств [1-4]. Основной задачей обеспечения безопасности информационных компьютерных систем является защита информации и ограничение круга лиц, имеющих доступ к этой критичной информации.

При организации вычислительных сетей важная роль отводится защите сообщений, передаваемых по сети с использованием того или иного алгоритма шифрования. Анализ существующих систем защиты информации [1-8] показал, что все множество алгоритмов можно разбить на две основные группы. Основу первой группы составляют симметричные алгоритмы шифрования, работающие с секретным ключом. В данных системах защиты информации от НСД ключ расшифрования совпадает с ключом зашифрования.

Вторая группа включает в себя асимметричные алгоритмы шифрования, работающие с открытым ключом [1; 3; 5-6]. В таких алгоритмах для зашифрования и расшифрования используются разные ключи, причем знание одного из них не дает практической возможности определить другой. Асимметричные системы во многих случаях обеспечивают наилучшее решение проблемы распределения ключей. Однако следует отметить, что алгоритмы асимметричных систем защиты информации от НСД настолько трудоемки по сравнению с обычными алгоритмами симметричного шифрования, что на практике рационально их использовать там, где объем шифрованной информации незначителен. Поэтому, с помощью алгоритмов ассиметричных систем целесообразно распределять ключи и осуществлять аутентификацию пользователей путем использования электронной подписи, а с помощью симметричных алгоритмов осуществлять обмен большими шифровальными потоками [4-5; 8].

Современные системы поблочного шифрования потока данных используются до 32 раундов перемешивания и рассеивания символов для обеспечения высокой стойкости шифра и статической равномерности символов (битов) в шифрованном тексте. Применение в таких системах операций подстановок, перестановок и циклического сдвига позволяет использовать стандартные микропроцессоры и реализовать аппаратные средства с требуемым быстродействием. Однако в таких системах имеет место распространения ошибок на всю длину блока и обеспечивается низкая скорость шифрования при программной реализации из-за большого количества шифрующих операций [1-4].

С появлением новых средств мультимедиа и сетей с высокой пропускной способностью, обеспечивающих передачу мультимедийных данных большого объема, в современных вычислительных системах начинают применяться технологии, осуществляющие обработку и передачу больших массивов. Для обеспечения интерактивного обмена данными такие системы должны работать в реальном масштабе времени. Поэтому процедура обеспечения конфиденциальности и целостности информации должна реализоваться с использованием поточных алгоритмов зашифрования. Для реализации эффективных методов поточного шифрования данных требуется разработка псевдослучайных последовательностей (ПСП). Такие псевдослучайные последовательности могут быть получены в рамках теории конечного поля с использованием регистров сдвига на базе многократных фильтров [1-2; 4; 6]

Системы побитого шифрования потока данных обеспечивают высокое быстродействие процессов шифрования и дешифрования информации, как аппаратных, так и программных средств защиты информации. Несмотря на то, что шифр, основанный на сложении потока псевдослучайных битов с битами исходного текста по модулю два, в общем случае теоретически нераспознаваем, сама система шифрования не отличается стойкостью и может быть мгновенно раскрыта при наличии определенного количества символов исходного и шифрованного текста. Уязвимость системы к атакам на основе исходных и подобранных текстов обусловлено тем, что при битовом шифровании потока данных сложение

символов по модулю два является единственным способом построения обратимой функции шифрования [6; 13].

Одним из наиболее перспективных способов защиты информации является применение систем поточного шифрования, использующие расширенные конечные поля GF(2v). Данные системы обладают более широкими возможностями по реализации различных криптографических функций обеспечения конфиденциальности и целостности информации. Применение различных операций, связанных со сложением, умножением, возведением в степень элементов конечного поля и их различных комбинаций позволяет реализовать адаптивные средства защиты информации, характеризующиеся высокой степенью информационной скрытности.

Нелинейное шифрование потока данных с операцией возведения в степень элемента конечного поля является одной из наиболее употребляемых криптографических процедур [1; 6-8]. Выбор данной процедуры обусловлен тем, что она нелинейна и для определения исходного текста по символам зашифрованного текста требуется вычисление дискретного логарифма [1; 3; 9-10]. Рассмотрим некоторые из них.

Как показано в [13] нелинейное шифрование потока данных можно реализовать с использованием операций сложения, умножения и возведения в степень элементов конечного поля, а также их комбинаций. При реализации нелинейного шифрования на основе операции сложения псевдослучайная последовательность элементов расширенного поля Галуа получается с помощью регистра сдвига, генерирующего двоичную ПСП. При этом двоичные числа снимаются одновременно с нескольких линий задержки на каждом такте работы регистра. Одновременно с регистра сдвига могут сниматься несколько псевдослучайных последовательностей элементов расширенного поля Галуа $\{x, y, \ldots\}$. Данные символы могут сниматься с разных ячеек генератора двоичного ПСП и в разной последовательности, поэтому будут создавать различные последовательности символов расширенного поля Галуа, причем каждая из них не будет циклически сдвинутой относительно других псевдослучайных последовательностей элементов.

Тогда символы шифрованного текста определяются в результате решения уравнения

$$\alpha(z) + y^{x_1}(z) \equiv \beta(z) \bmod \pi(z), \qquad (1)$$

где $x_1$ – целое число, которое выбирается заранее и используется постоянно или меняется на каждом такте работы регистра сдвига; $y(z)$ – полиномиальное представление псевдослучайной последовательности элементов поля Галуа; $\alpha(z)$ – символы исходного сообщения, представленные в полиномиальном виде; $\mathrm{ord}(\alpha(z)) < \mathrm{ord}\pi(z)$ – степень полинома $\alpha(z)$; $\beta(z)$ – полиномиальное представление шифрованного сообщения; $\pi(z)$ – порождающий полином.

Дешифрование сообщений осуществляется путем решения уравнения

$$\beta(z) + (\pi(z) + y^{x_1}(z)) \bmod \pi(z) \equiv \alpha(z), \qquad (2)$$

где «+» – суммирование по модулю два.

В этом случае на приемной стороне вычисляется псевдослучайная последовательность символов $\pi(z) + y^{x_1}(z)$, сопряженная по отношению к псевдослучайной последовательности символов $y^{x_1}(z)$.

При реализации нелинейного шифрования на основе операции умножения для шифрования символов исходного текста могут использоваться символы псевдослучайной последовательности конечного поля, возведенные в степень $x_1$. Аналогично, как и в предыдущем случае, $x_1$ может быть постоянным числом или переменным, изменяемым по квазислучайному закону на каждом такте работы регистра сдвига или через определенное число тактов работы регистра сдвига. При этом зашифрованное сообщение определяется выражением

$$\alpha(z) y(z)^{x_1} \equiv \beta(z) \bmod \pi(z). \qquad (3)$$

Процедура дешифрования определяется следующим соотношением

$$\beta(z)(y^{x_1}(z))^{-1} \equiv \alpha(z) \bmod \pi(z), \qquad (4)$$

где $(y(z)^{x_1})^{-1} \bmod \pi(z)$ – обратная величина функции $y(z)^{x_1}$ по модулю $\pi(z)$.

В работе [13] показаны нелинейное шифрование потока данных с операцией возведения в степень символов конечного поля. В этом случае для шифрования поступающих на вход символов исходного текста, представленного в полиномиальной форме $\alpha(z)=\{\alpha_j(z)\}$ вычисляются значения символов псевдослучайной последовательности конечного поля $x=\{x_j\}$ на различных текстах работы регистра сдвига $j = 0; 1; 2 \ldots$ и определяются символы шифрованного сообщения

$$\alpha(z)^{x} \equiv \beta(z) \bmod \pi(z). \qquad (5)$$

Однако операция возведения элемента поля в степень трудоемка и требует больших затрат машинного времени. Для сокращения времени выполнения этой процедуры целесообразно перейти к обработке данных, представленных в полиномиальной системе классов вычетов (ПСКВ). Основные принципы построения этих непозиционных кодов, а также схемные реализации вычислительных устройств, функционирующих в ПСКВ, представлены в работах [11-12].

В этом случае поток входных битов разбивается на отдельные блоки. Каждый такой блок A двоичного кода представляется в полиномиальной форме A(z), причем степень данного полинома не должна превышать степень выбранного рабочего диапазона

$$P(z) = \prod_{i=1}^{n} p_i(z), \qquad (6)$$

то есть удовлетворять условию

$$\mathrm{ordA}(z) < \mathrm{ordP}(z), \qquad (7)$$

где $p_i(z)$ – неприводимый полином; i = 1; 2 … n.

Тогда полином A(z), имея максимальную степень $\mathrm{ordP}(z)-1$, может быть представлен следующим образом:

$$A(z) = l_{\mathrm{ordP}(z)-1} z^{\mathrm{ordP}(z)-1} + l_{\mathrm{ordP}(z)-2} z^{\mathrm{ordP}(z)-2} + \ldots + l_1 z^1 + l_0 z^0, \qquad (8)$$

где $l_k \in \{0;1 \ldots p-1\};\ k = 0;1 \ldots \mathrm{ord}\pi(z)-1.$

Исходя из условия построения системы криптографической защиты информации в расширенных полях Галуа на основе полиномиальной системы класса вычетов, имеем, что рабочий диапазон P(z) представляет собой кольцо неприводимых полиномов $p_i(z),\ i = 1;2 \ldots n$, то есть определяется согласно выражению (6).

В этом случае, используя изоморфизм, порожденный китайской теоремой об остатках, а также учитывая условие (7), можно отметить, что каждый блок A(z), представленный в полиномиальной форме, однозначно представляется в виде набора остатков по выбранным основаниям $p_i(z)$

$$A(z) = (\alpha_1(z), \alpha_2(z) \ldots \alpha_n(z)). \qquad (9)$$

При этом значение остатков будут заданы

$$\alpha_i(z) = (l_{\mathrm{ordP}(z)-1} z^{\mathrm{ordP}(z)-1} + l_{\mathrm{ordP}(z)-2} z^{\mathrm{ordP}(z)-2} + \ldots + l_1 z^1 + l_0) \bmod p_i(z); \qquad (10)$$

где i = 1; 2 … n.

Для реализации алгоритма нелинейного шифрования с возведением в степень в расширенных полях Галуа $GF(p^v)$ необходимо возвести j-ый блок $A_j(z)$ в степень X по модулю P(z)

$$\beta_j(z) = A_j^{X_j}(z) \bmod P(z), \qquad (11)$$

где j = 0; 1; 2; 3 …

Значение X снимается с выходов линии задержки многотактового фильтра, генерирующего псевдослучайную последовательность. Структура многотактового фильтра будет определяться характеристическим многочленом $\rho(z)$. Так как псевдослучайная последовательность может сниматься одновременно с выходов нескольких линий задержки, то желательно, чтобы степень порождающего полинома $\rho(z)$ была значительно больше величины $p^v - 1$. Это позволит при определенных условиях нарушить детерминированные свойства ПСП. При этом последовательности X, снимаемые с выходов разных линий задержки, не будут коррелированны друг с другом, что, в конечном итоге, позволит повысить степень криптографической защиты.

Двоичный поток псевдослучайной последовательности X разбивается на блоки вида $X = \{x_0; x_1; x_2 \ldots\}$, при этом каждый блок содержит не более чем $p^v - 1$ двоичных разряда. Данные блоки поступают на шифратор для реализации процедуры нелинейного шифрования согласно выражению (11). Так как блок $A_j(z)$ представляется в виде набора остатков $\alpha_i(z)$, то справедливо следующее равенство

$$\beta_j(z) = A_j^{X_j}(z) \bmod P(z) = ((\alpha_1^j(z), \alpha_2^j(z) \ldots \alpha_n^j(z))^{X_j} \bmod P(z), \qquad (12)$$

где $\alpha^j(z) \equiv A_j(z) \bmod p_i(z)$.

Так как сравнения по одному и тому же модулю можно почленно умножать, то последнее выражение представляется в виде:

$$\beta_j(z) = ((\alpha_1^j)^{x_j}(z), \ldots, (\alpha_n^j)^{x_j}(z)) \bmod P(z). \qquad (13)$$

Таким образом, операция возведения в степень по модулю P(z), являющаяся основой разработанного алгоритма нелинейного шифрования, сводится к совокупности операций возведения в степень остатков $\alpha_i(z)$ по соответствующим основаниям $p_i(z)$.

На рис. 1 представлена структура нелинейного шифратора, функционирующего в полино-

миальной системе классов вычетов. Исходный полином A(z) поступает на входы блоков, осуществляющих прямое преобразование из позиционного кода в ПСКВ (ПСС-ПСКВ). Полученные остатки $\alpha_i^j(z)$, i = 1; 2 … N, подаются на входы преобразователей «элемент-индекс» (Элеминд). С выходов данных преобразователей индексы в двоичном коде поступают на первые входы умножителей (Умн) по модулю $p^{ordp_i(z)} - 1$, где p – характеристика поля, $ordp_i(z)$ – степень i-го основания ПСКВ. На вторые входы поступает блок $X_j$, снимаемый с выхода генератора ПСП. Результаты произведения выдаются на входы преобразователей «индекс-элемент» (Инд-элем). На выходах этих преобразователей в двоичном коде получаются остатки зашифрованного сообщения, согласно (12).

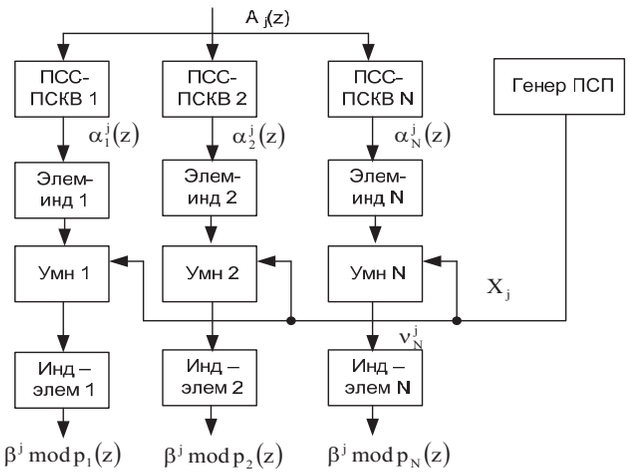


Рис. 1. Структура нелинейного шифратора, функционирующего в ПСКВ

Если i-ый остаток j-го блока отличен от нуля, то есть $\alpha_i^j(z) \neq 0$, то он входит в состав мультипликативной группы, порождаемой неприводимым полиномом $p_i(z)$, взятым в состав оснований полиномиальной системы классов вычетов. Следовательно, при возведении в степень ненулевого элемента мультипликативной группы будет получен другой элемент этой группы, который является циклически сдвинутым на $x_j$ разрядов влево.

В результате выполнения процедур нелинейного шифрования с использованием операции возведения в степень образуется кольцо, в котором будет отсутствовать делитель нуля. Таким образом, будет получена область целостности или целостное кольцо.

Если i-ый остаток j-го блока $A_j(z)$ равен нулю, то при возведении в любую степень данный остаток будет равен также нулю.

Следует отметить, что если информацию о последовательности $X = \{x_0; x_1; x_2 \ldots\}$ снимать с выхода одной линии задержки многотактового фильтра, то может возникнуть ситуация, когда j-ый блок будет равен нулю. В этом случае целесообразно заменить нулевое значение блока $x_j$ на значение $p^v - 2$. При этом такая замена должна осуществляться, соответственно, как на передающей стороне, так и на принимающей. Введение числа $p^v - 2$ вместо $x_j = 0$ позволит обеспечить выполнение функции, обратной процедуре зашифрования, которая осуществлялась в шифраторе.

На приемной стороне осуществляется процедура расшифрования согласно

$$A_j(z) = \sqrt[x_j]{\beta_j(z)} \bmod P(z). \qquad (14)$$

Исходя из условия, что операции выполняются в кольце полинома P(z), то справедливо

$$\alpha_i^j(z) = \sqrt[x_j]{\beta_i^j(z)} \bmod p_i(z), \qquad (15)$$

где $\beta_i^j(z) \equiv \beta_j(z) \bmod p_i(z)$.

Очевидно, что применение параллельной обработки данных позволяет за счет выполнения мультипликативных операций с малоразрядными остатками повысить скорость зашифрования данных.

Рассмотрим процедуру расшифрования, выполняемую также с использованием полиномиальной системы. Как отмечалось ранее, для выполнения процедуры дешифрования используется выражение (15). Для вычисления корня степени $x_j$ из $\beta_j$ необходимо свести данную немодульную операцию к совокупности модульных. Исходя из условия

$$x_j (x_j)^{-1} \equiv 1 \bmod p^v - 1, \qquad (16)$$

необходимо определить мультипликативную обратную величину $(x_j)^{-1}$ относительно $x_j$ по модулю $p^v - 1$. Для этого необходимо на приемной стороне использовать блок, позволяющий вычислить данную величину по значению $x_j$, поданному с выхода многотактового фильтра.

Рассмотрим пример реализации нелинейного шифрования в полиномиальной системе классов вычетов поле $GF(2^3)$. В данном поле определены два неприводимых полинома третьей степени и один полином первой степени. Таким образом, данная система шифрования содержит следующие основания:

$$p_1(z) = z + 1,$$
$$p_2(z) = z^3 + z^2 + 1,$$
$$p_3(z) = z^3 + z + 1.$$

Произведение данных неприводимых полиномов образует рабочий диапазон, который

$$P(z) = \prod_{i=1}^{3} p_i(z) = z^7 + 1.$$

Следовательно, для выполнения процедур нелинейного шифрования на основе возведения в степень по модулю с использованием ПСКВ необходимо поток битовой информации разбивать на блоки, содержащие по 7 бит каждый.

Пусть задана двоичная последовательность двоичных битов

00111101100011000111 1.

Данная последовательность будет представлена в виде следующего набора блоков:

$A_1 = 0011110;$
$A_2 = 1100011;$
$A_3 = 0001111.$

Представим эту последовательность блоков в полиномиальной форме. Получаем

$$A_1(z) = z^4 + z^3 + z^2 + z;$$
$$A_2(z) = z^6 + z^5 + z + 1;$$
$$A_3(z) = z^3 + z^2 + z + 1.$$

Полученные значения поступают на входы модуля прямого преобразования двоичного позиционного кода в непозиционный код. Тогда блок $A_1(z)$ в полиномиальной системе классов вычетов будет иметь вид

$$A_1(z) = z^4 + z^3 + z^2 + z = (0, z^2, z + 1).$$

Остальные блоки открытого текста представляются аналогичным образом:

$$A_2(z) = z^6 + z^5 + z + 1 = (0,\ z^2 + z,\ 1);$$
$$A_3(z) = z^3 + z^2 + z + 1 = (0, z, z^2).$$

Чтобы повысить криптостойкость алгоритма нелинейного шифрования с использованием операции возведения в степень по модулю, предлагается снимать ПСП параллельно с выходов $\nu$ различных линий задержек генератора ПСП. Пусть двоичная последовательность двоичных разрядов в параллельном коде снимаемая с выходов трех линий задержек имеет вид

$$X = \{101, 110, 111, \ldots\},$$

что соответствует числам

$$X_5 = \{5, 6, 7, \ldots\}.$$

Так как $7 = 0 \bmod 2^3 - 1$, то, как отмечалось ранее, это число меняем на $p^{\nu} - 2 = 2^3 - 2 = 6$. В результате получаем последовательность

$$X^* = \{5, 6, 6, \ldots\}.$$

Полученная последовательность X* представляет собой показатели степеней, в которые необходимо возвести значение $A_j(z)$, представленных в модулярном коде ПСКВ. Произведем криптографическое преобразование для блока $A_1(z)$. Получаем

$$\beta_1(z) = A_1^5(z) = (z^4 + z^3 + z^2 + z)^5 \bmod z^7 + 1 =$$
$$= z^6 + z^5 = 1100000.$$

Представим полученный результат в полиномиальной системе класса вычетов

$$\alpha_1(z) = A_1^5(z) \bmod p_1(z) = \left| z^6 + z^5 \right|_{z+1}^{+} = 0,$$
$$\alpha_2(z) = A_1^5(z) \bmod p_2(z) = \left| z^6 + z^5 \right|_{z^3+z^2+1}^{+} = z^2 + 1,$$
$$\alpha_3(z) = A_1^5(z) \bmod p_3(z) = \left| z^6 + z^5 \right|_{z^3+z+1}^{+} = z.$$

Следовательно,

$$A_1^5(z) = z^6 + z^5 = (0, z^2 + 1, z).$$

Выполним процедуру нелинейного шифрования в ПСКВ:

$$\beta_1(z) = A_1^5(z) = (z^4 + z^3 + z^2 + z)^5 \bmod z^7 + 1 =$$
$$= \left(\left|0^5\right|_{z+1}^{+}, \left|(z^2)^5\right|_{z^3+z^2+1}^{+}, \left|(z+1)^5\right|_{z^3+z+1}\right) =$$
$$= (0,\ z^2 + 1,\ z).$$

Проведем криптографические преобразования с остальными блоками открытого текста. Для второго блока открытых данных получаем

$$\beta_2(z) = A_2^6(z) = \left|(z^6 + z^5 + z + 1)^6\right|_{z^7+1}^{+} =$$
$$= z^6 + z^2 = 1000100.$$

В полиномиальной системе класса вычетов данный результат получается в виде

$$\beta_2(z) = A_2^6(z) = z^6 + z^2 = (0, z, 1) = (0{,}010{,}001).$$

Реализуем процедуру нелинейного шифрования в полиномиальной системе класса вычетов

$$\beta_2(z) = A_2^6(z) = (z^6 + z^5 + z + 1)^6 \bmod z^7 + 1 =$$
$$= (\left|0^6\right|_{z+1}^{+}, \left|(z^2 + z)^6\right|_{z^3+z^2+1}^{+}, \left|1^6\right|_{z^3+z+1}^{+}) = (0, z, 1) =$$
$$= (0, 010, 001).$$

Для третьего блока открытых данных вычислим значение зашифрованных данных:

$$\beta_3(z) = A_3^6(z) = \left|(z^3 + z^2 + z + 1)^6\right|_{z^7+1}^{+} =$$
$$= z^4 + 1 = 0010001.$$

Представим полученный результат в ПСКВ

$$\beta_3(z) = A_3^6(z) = \left|(z^3 + z^2 + z + 1)^6\right|_{z^7+1}^{+} =$$
$$= z^4 + 1 = 0010001.$$

Воспользуемся математическим аппаратом полиномиальной арифметики для выполнения процедур шифрования. Получаем

$$\beta_3(z) = A_3^6(z) = (z^3 + z^2 + z + 1)^6 \bmod z^7 + 1 =$$
$$= (\left|0^6\right|_{z+1}^{+}, \left|z^6\right|_{z^3z^2+1}^{+}, \left|(z^2)^6\right|_{z^3+z+1}^{+}) =$$
$$= (0, z^2 + z, z^2 + z + 1) = (0,110,111).$$

Полученный результат свидетельствует о возможности применения полиномиальной системы класса вычетов при реализации алгоритма нелинейного шифрования с использованием операции возведения в степень по модулю.

Очевидно, что применение параллельной обработки данных позволяет за счет выполнения мультипликативных операций с малоразрядными остатками повысить скорость зашифрования данных.

Рассмотрим процедуру расшифрования, выполняемую также с использованием полиномиальной системы. Как отмечалось ранее, для выполнения процедуры дешифрования используется выражение (14). Для вычисления корня степени $x_j$ из $\beta_j$ необходимо свести данную немодульную операцию к совокупности модульных. Исходя из условия (16), необходимо определить мультипликативную обратную величину $(x_j)^{-1}$ относительно $x_j$ по модулю $p^v - 1$. Для этого необходимо на приемной стороне использовать блок, позволяющий вычислить данную величину по значению $x_j$, поданному с выхода многотактового фильтра. В представленном примере для расширенного поля Галуа $GF(2^3)$ значения $X^{-1}$ будут иметь следующий вид

$$X^{-1} = \{3, 6, 6, \ldots\}.$$

Осуществим операцию дешифрования с использованием и без полиномиальной системы классов вычетов.

Итак, полученный первый блок $\beta_1(z)$ длиной 7 бит поступает на устройство, реализующее операцию дешифрования согласно (14). При этом с выхода блока вычисления обратной мультипликативной величины подается значение $X_1^{-1} = 3$ в двоичном коде. В результате выполнения операции по модулю P(z) получаем:

$$A_1(z) = \sqrt[x_1]{\beta_1(z)} \bmod P(z) =$$
$$= (z^6 + z^5)^{-x_1} \bmod z^7 + 1 = (z^6 + z^5)^3 \bmod z^7 + 1 =$$
$$= z^4 + z^3 + z^2 + z = (0, z^2, z + 1).$$

Реализуем процедуру дешифрования $\beta_1(z)$ в полиномиальной системе классов вычетов:

$$A_1(z) = \sqrt[x_1]{(0, z^2 + 1, z)} \bmod P(z) = \left|(0, z^2 + 1, z)^3\right|_{z^7+1}^{+} =$$
$$= (\left|0^3\right|_{z+1}^{+}, \left|(z^2 + 1)^3\right|_{z^3+z^2+1}^{+}, \left|z^3\right|_{z^3+z+1}^{+}) =$$
$$= (0, z^2, z + 1).$$

Аналогичным образом поступаем с последующими блоками зашифрованных данных $\beta_1(z)$, $\beta_2(z)$, $\beta_3(z)$.

Для блока $\beta_2(z)$ получаем

$$A_2(z) = \sqrt[x_2]{\beta_2(z)} \bmod P(z) = \left|(z^6 + z^2)^{-x_2}\right|_{z^7+1}^{+} =$$
$$= \left|(z^6 + z^2)^6\right|_{z^7+1}^{+} = z^6 + z^5 + z + 1 = (0, z^2 + z, 1).$$

Воспользуемся полиномиальной системой класса вычетов для выполнения процедуры дешифрования

$$A_2(z) = \sqrt[x_2]{(0, z, 1)} \bmod P(z) = \left|(0, z, 1, z)^6\right|_{z^7+1}^{+} =$$
$$= (\left|0^6\right|_{z+1}^{+}, \left|z^6\right|_{z^3+z^2+1}^{+}, \left|1^6\right|_{z^3+z+1}^{+}) = (0, z^2 + z, 1).$$

Проведем дешифрование блока $\beta_3(z) = z^4 + 1$:

$$A_3(z) = \sqrt[x_3]{\beta_3(z)} \bmod P(z) = \left|(z^4 + 1)^{-x_3}\right|_{z^7+1}^{+} =$$
$$= \left|(z^4 + 1)^6\right|_{z^7+1}^{+} = z^3 + z^2 + z + 1 = (0, z, z^2)$$

При реализации дешифрования в полиномиальной системе класса вычетов получаем

$$A_3(z) = \sqrt[x_3]{\beta_3(z)} \bmod P(z) =$$
$$(0, z^2 + z, z^2 + z + 1)^6 \bmod z^7 + 1 =$$
$$= (\left|0^6\right|_{z+1}^{+}, \left|(z^2 + z)^6\right|_{z^3+z^2+1}^{+}, \left|(z^2 + z + 1)^6\right|_{z^3+z+1}^{+}) =$$
$$= (0, z, z^2).$$

Полученные результаты свидетельствуют о том, что при применении полиномиальной системы класса вычетов получается результат, аналогичный операции нелинейного шифрования с возведением в степень по модулю.

В ходе проведенных исследований было выявлено, что применение полиномиальной системы классов вычетов для реализации нелинейного шифрования позволило снизить временные затраты на 9,2% по сравнению с выполнением метода шифрования с возведением в степень по модулю в поле Галуа $GF(2^3)$. Следует отметить, что при увеличении разрядности обрабатываемых данных возрастает эффективность применения полиномиальной системы классов вычетов для реализации нелинейных криптографических процедур защиты данных от НСД.

## Выводы

Проведенные исследования показали, что системы поточного шифрования, использующие расширенные конечные поля, обладают более широкими возможностями по реализации различных криптографических функций обеспечения конфиденциальности и целостности информации. Применение в таких функциях различных операций, связанных со сложением, умножением, возведением в степень символов в конечном поле и их различных комбинаций и использование возможности генерации в конечном поле множества различных псевдослучайных последовательностей максимальной длины позволяет реализовать такие защиты информации, для которых наличие исходного и шифрованного текста не снижает криптостойкость системы. При этом применение полиномиальной системы классов вычетов позволяет повысить скорость выполнения процедур нелинейного шифрования.

## Литература


1. Шнайдер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Изд. ТРИУМФ, 2003. – 816 с.
2. Столингс В. Криптография и защита сетей: принципы и практика. Пер с англ. М.: Изд. дом «Вильямс», 2001. – 672 с.
3. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999. – 109 с.
4. Введение в криптографию. Под ред. В.В. Ященко. М.: МЦНМО «ЧеРо», 1999. – 272 с.
5. Чмора А.П. Современная прикладная криптография. М.: Гелиос АРВ, 2002. – 256 с.
6. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.
7. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.
8. Зензин О.С., Иванов М.А. Стандарт криптографической защиты AES. Конечные поля. М: КУДИЦ-ОБРАЗ, 2002. – 176 с.
9. Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах. М.: Сов. радио, 1968. – 440с.
10. Глухов М.М., Елизаров В.П., Нечаева А.А. Алгебра. Т. 2. М.: Гелиос АРВ, 2003. – 414 с.
11. Червяков Н.И., Калмыков И.А., Галкина В.А. и др. Элементы компьютерной математики и нейроноинфроматики. Под ред. Н.И. Червякова. М.: Физматлит, 2003. – 216 с.
12. 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.
13. Калмыков И.А., Кихтенко О.А., Барильская А.В. Устройство для вычисления индекса элементов поля Галуа по модулю. Материалы НТК «Современные телекоммуникационные и информационные технологии». Июнь, 2007. http://www.rae.ru/zk


## NONLINEAR TECHNOLOGY DATA ENCRYPTION IN HIGH-SPEED COMMUNICATION NETWORKS

**Kalmikov I.A., Strekalov Y.A., Shelkunova Y.O., Kihtenko O.A., Barilskay A.V.**

**The article considered the technology of constructing nonlinear cryptosystem encryption using polynomial system of residue classes. Propose a method to provide high speed encryption of data flow.**

***Keywords:*** *nontraditional algorithms of encryption, fields of Galois, polynomial system of residue classes, nonlinear data encryption.*

Калмыков Игорь Анатольевич, д.т.н., профессор Кафедры «Общематематические и естественнонаучные дисциплины» Ставропольского филиала (СФ) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ), г. Ставрополь. E-mail: kia762@yandex.ru

Стрекалов Юрий Анатольевич, к.т.н., доцент СФ ПГУТИ. E-mail: pgati@statel.stavropol.ru

Щелкунова Юлия Олеговна, к.т.н., доцент Ставропольского военного института ракетных войск. Тел. (8-8652) 39-73-34. E-mail: sfpgati@yandex.ru

Кихтенко Ольга Алексеевна, аспирант Кафедры «Защита информации» Северо-Кавказский государственного технического университета (СВКГТУ), г. Ставрополь. Тел. (8-8652) 95-65-46. E-mail: sfpgati@yandex.ru

Барильская Анастасия Владимировна, 1987 г.р., аспирант Кафедры «Защита информации» СВКГТУ. Тел. (8-8652) 95-65-46. E-mail: sfpgati@yandex.ru

## ТЕХНОЛОГИИ ТЕЛЕКОММУНИКАЦИЙ

УДК 621.396.2

# ИССЛЕДОВАНИЕ ДЕФЕКТОВ ПРОФИЛЯ ПОКАЗАТЕЛЯ ПРЕЛОМЛЕНИЯ МНОГОМОДОВЫХ ОПТИЧЕСКИХ ВОЛОКОН КАБЕЛЕЙ СВЯЗИ

*Бурдин А.В., Яблочкин К.А.*

В работе представлены результаты измерений профилей показателя преломления образцов кварцевых градиентных многомодовых оптических волокон (МОВ) разных поколений. Выявлены и классифицированы характерные технологические дефекты профилей исследуемых образцов ОВ. Получены оценки параметров данных дефектов. Приведены результаты сопоставления протоколов измерения профилей и дифференциальной модовой задержки (ДМЗ) для этих же волокон. Представлены данные анализа влияния дефектов профиля градиентных МОВ на ДМЗ.

***Ключевые слова:*** многомодовое оптическое волокно, дифференциальная модовая задержка, градиентный профиль показателя преломления, дефекты профиля показателя преломления.

### Введение

Значительные достижения технического прогресса в области систем и сетей хранения данных (SAN), реорганизация структуры центров обработки данных (ЦОД) и вычислительных центров (ВЦ) – замена мэйнфреймов на распределенные серверные кластеры, объединенные в мультигигабитные инфокоммуникационные сети, наконец, развитие, расширение и интеграция корпоративных локальных информационно-вычислительных сетей (LAN) являются одним из ключевых факторов стимулирования совершенствования техники и технологии многомодовых волоконно-оптических линий передачи (ВОЛП). Вышесказанное, например, относится и разработке многомодовых оптических волокон с улучшенными характеристиками категорий OM3 и OM4. В свою очередь, это делает данные технологии привлекательными для решения более широкого круга задач, включая реконструкцию и увеличение пропускной способности уже введенных в эксплуатацию линий передачи инфокоммуникационных сетей с МОВ разных поколений.

Как известно, пропускная способность МОВ ограничивается дифференциальной модовой задержкой, которая во многом определяется степенью отклонения профиля показателя преломления МОВ от идеального, то есть, параметрами дефектов профиля [1]. Для эффективного использования МОВ, корректного применения известных решений и разработки новых способов подавления ДМЗ нужны данные этих параметров. Вместе с тем в открытой печати сведения о дефектах профилей МОВ ограничены и носят общий характер. В технической литературе и спецификациях МОВ количественные оценки параметров дефектов профиля отсутствуют, как правило, приводится описание идеального профиля [2].

В данной работе представлены результаты измерений профиля показателя преломления образцов МОВ разных поколений, выявлены и классифицированы дефекты профилей, даны их количественные оценки. Приведены результаты сопоставления с протоколами измерения ДМЗ тестируемых образцов МОВ, что позволило в первом приближении оценить зависимость ДМЗ МОВ от параметров дефектов профиля.

### Подготовка образцов МОВ

На предварительной стадии было отобрано 14 образцов градиентных МОВ 50/125, которые впоследствии условно сгруппировали по приблизительным датам выпуска. В группу «I» (7 шт.) вошли семь образцов многомодовых световодов первого поколения середины 80-х годов отечественного производства (г. Мытищи). В группу