УДК 681.3.06

С.О. Мартыненко, В.А. Краснобаев

Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Харьков

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ КОДОВ МОДУЛЯРНОЙ СИСТЕМЫ СЧИСЛЕНИЯ ДЛЯ СОЗДАНИЯ СИСТЕМЫ ОБРАБОТКИ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ РЕАЛЬНОГО ВРЕМЕНИ

В статье проводятся теоретические исследования возможности эффективного применения модулярной системы счисления для обработки криптографической информации над конечным полем в реальном времени. Результаты проведенных исследований рекомендуются для обработки криптопреобразований, основанных на арифметике в группе точек эллиптических кривых.

Ключевые слова: *система обработки криптографической информации, модулярная система счисления, цифровая обработка сигналов, поля Галуа, арифметические операции по модулю.*

Введение

В нашей стране практически создана и используется общегосударственная инфраструктура открытых ключей, которая используется для поддержки электронной цифровой подписи. В этом плане весьма актуальной и до конца нерешенной задачей является задача эффективной обработки цифровых сигналов (ЦОС) в системах обработки криптографической информации (СОКИ) реального времени. В частности, актуальны исследования, посвященные вопросам эффективной реализации криптопреобразований на гиперэллиптических кривых. С одной стороны, ЦОС занимает основополагающее место в современных средствах переработки информации в связи с такими ее преимуществами, как высокая точность обработки информации и гибкость. С другой стороны, эффективность ЦОС в большей степени определяется объемом необходимых вычислений, который получается при реализации математических моделей (ММ) СОКИ. Реализация задач ЦОС заключается в синтезе ММ функционирования данной системы и далее ее технической реализации. Практическая реализация задач ЦОС наталкивается на ряд трудностей. Это обусловлено двумя основными факторами: во-первых, нет четкого, единого подхода к синтезу математических моделей систем ЦОС; во-вторых, недостаточная теоретическая и практическая проработка вопросов создания высокопроизводительных СОКИ, реализующих математические модели систем реального времени.

Анализ последних исследований и публикаций. В последнее время получают распространение математические модели СОКИ, созданные на основе применения абстрактных алгебраических систем, в частности, математические модели можно определить как кривую над конечным полем с элементами меньшей размерности, что является альтернативой криптопреобразованием на эллиптических кривых. Это возможно на основании применения теории полей Галуа [1, 2]. Основные преимущества данных моделей систем ЦОС состоят в следующем:

– такие модели более полно учитывают дискретную структуру представления обрабатываемого цифрового сигнала;

– упрощается аппаратная реализация математических моделей.

Основной недостаток математических моделей систем ЦОС, созданных на основе использования абстрактных алгебраических систем, состоит в необходимости разработки принципиально новой структуры СОКИ для эффективной реализации операций конечного поля Галуа или кольца с заданной алгебраической структурой. В связи с этим перечислим основные специфические требования и характерные особенности, предъявляемые к СОКИ реального времени:

– необходимость обработки большого количества информации в реальном времени, что требует сверхвысокого быстродействия (высокой пользовательской производительности) решения задач СОКИ, а это, в свою очередь, обуславливает необходимость обеспечения высокой надежности (отказоустойчивости) функционирования и достоверности вычислений;

– универсальность для заданного класса криптографических задач;

– необходимость оперирования с целыми числами, являющимися элементами поля Галуа GF(M) или конечного кольца вычетов;

– эффективная реализация операции основного поля, над которым определена кривая (к ним относятся операции модульного сложения, умножения и возведения в квадрат по модулю);

– отсутствие привычного физического смысла

промежуточных результатов вычислений в конечных полях или кольцах, что одновременно с требованием использования полей Галуа GF(M) с большим значением модуля M, обуславливает необходимость использования СОИ с сравнительно большой разрядной сеткой;

– глубокая адаптация к классу (типу) решаемых криптографических задач (к типу операций, входящих в реализуемые алгоритмы), что сопровождается необходимостью создания рациональных структуру СОКИ, а это, в свою очередь, может оказать существенное влияние на такие характеристики СОКИ, как производительность, отказоустойчивость, надежность, также на конструкцию отдельных функциональных блоков и узлов, входящих в ее состав;

– адаптация к отказам и сбоям;

– в отдельных случаях (специализированные СОКИ), жесткие требования к массогабаритным характеристикам, потребляемой мощности и т.п.

Анализ методов и алгоритмов решения криптографических задач посредством СОКИ, функционирующих в позиционной системе счисления (ПСС), показал, что, во-первых, возможности позиционных систем счисления для построения СОКИ различного назначения практически ограничены, и, во-вторых, на современном уровне развития технологии применение позиционных вычислителей не может полностью обеспечить требований, предъявляемых к средствам обработки информации [3]. Вследствие этого возникает задача поиска путей совершенствования СОКИ на основе использования нетрадиционных систем счисления наиболее адаптивных к классу задач, решаемых системами ЦОС. Одной из таких систем счисления может служить модулярная арифметика (МА), т.е. непозиционная система счисления в остаточных классах (СОК), или модулярная система счисления (МСС).

Пусть для области определения E_N цифрового сигнала $x(n)$ рассмотрим абелеву группу $H = H_1 \times H_2 ... \times H_n$, где H – циклическая группа порядка $H:1 .N = \sum_{i=1}^{n} q_i;\ q_i = m_i^{\alpha i}$ – порядок подгруппы H_i; m_i – набор простых чисел ($i = \overline{1,n}$) $\alpha_i \in Z$, где Z – кольцо целых чисел.

Произвольный элемент $n \in H$ может быть представлен в виде $n = n_1, n_2, ..., n_i, ..., n_\varsigma$; $n_i \in H_i$. В этом случае групповая операция определяется следующим образом:

$$Z = x \oplus y = x_1, x_2, ..., x_n \oplus (y_1, y_2, ..., y_n) =$$
$$x_1 \oplus y_1 , (x_2 \oplus y_2 , ..., (x_n \oplus y_n)),$$

где $x_i \oplus y_i = Z_i (\mathrm{mod}\, h_i)$, h_i – порядок подгруппы H_{hi}; $x = (x_1, x_2, ..., x_n) \in H$, $x_i = H_i$; H – циклическая неразложимая группа порядка $H:1 = m_i^{\alpha i} = h_i$ (при $\alpha_i = 1 \to m_i = h_i$).

Рассмотрим общий случай представления групп, когда группа равна прямой сумме подгрупп вида

$$H = H_{h_1} \oplus H_{h_2} \oplus ... \oplus H_{h_n}, \text{ где } H:1 = \prod_{i=1}^{n} m_i^{\alpha i},$$

где h_i – порядок подгруппы H_{h_i}; для $i = \overline{1,n}$.

Известно, что сумма $H_{h_1} \oplus H_{h_2} \oplus ... \oplus H_{h_n}$ называется прямой суммой, если каждое слагаемое имеет нулевое переназначение с суммой остальных, т.е.

$$(H_{h_1} + H_{h_2} + ... + H_{h_{i-1}} + H_{h_{i+1}} + ... + H_{h_n}) \bigcap H_{h_n} = 0$$

для $i = \overline{1,n}$.

Известно, что всякая конечная абелева группа изоморфна внешней прямой сумме примарных циклических групп. Пусть $H = H_1 \oplus H_2 \oplus ... \oplus H_n$ – прямая сумма. Тогда,

$$H = H_1 \oplus ... \oplus H_{i-1} \oplus H_i \oplus ... \oplus H_n$$

для $i = \overline{1,n}$, и если

$$H = H_1 \oplus ... \oplus H_n,\ H_i = H_{i_1} \oplus ... \oplus H_{i_{k_i}}$$

для $i = \overline{1,n}$, то

$$H = H_{11} \oplus ... \oplus H_{1k_1} \oplus H_{21} \oplus ...$$
$$\oplus H_{2k_2} \oplus ... \oplus H_{n_1} \oplus ... \oplus H_{nk_n},$$

где H_{ik_i} – подмодули.

В этом случае, если $M = \prod_{i=1}^{n} m_i$ и $HOD(m_i, m_j) = 1$, а $i \neq j$, то кольцо Z_M классов вычетов по модулю M изоморфно прямой сумме $GF\ m_1 + GF\ m_2 + ... + GF\ m_i + ... + GF\ m_n$ конечных полей Галуа вида $GF\ m_i$, для $i = \overline{1,n}$. Отметим известное теоретическое положение, что всякая циклическая группа изоморфна или группе целых чисел по сложению или группе вычетов по некоторому модулю M. Зададим изоморфизм φ между Z_M и прямой суммой $\sum_{i=1}^{n} GF\ m_i$ конечных полей Галуа в виде $\varphi: a \to (a_1, a_2, ...a_n)$, где $a \in Z_M$, $a_i = a(\mathrm{mod}\, m_i)$, где $i = \overline{1,n}$, причем обратное преобразование представим в виде $\varphi^{-1}: (a_1, a_2, ...a_n) \to a$.

Пусть N делит $m_i - 1$ для $i = \overline{1,n}$. Тогда существует примитивный корень ξ_i из единицы $GF\ m_i$. Элемент $\varphi^{-1}: (\xi_1, \xi_2, ..., \xi_n) \to \xi$ соответствует примитивному корню N – й степени из еди-

ницы в Z_M. Отсюда следует, что в N точках существует прямое и обратное преобразование над Z_M, т.е.

$$S\ a\ = \sum_{n=0}^{N-1} x\ n\ \xi^{-an}, \qquad (1)$$

$$x(n) = N^{-1}\sum_{a=0}^{N-1} S(a)\xi^{an}. \qquad (2)$$

Применяя преобразование φ, получим следующие соотношения:

$$\varphi\left[S\ a\ \right] = \sum_{n=0}^{K-1} \varphi\left[x\ n\ \right]\varphi\left[\xi^{-an}\right],$$

$$\varphi\left[x\ n\ \right] = N^{-1}\sum_{a=0}^{N-1} \varphi\left[S\ a\ \right]\varphi\left[\xi^{an}\right],$$

т.е . $S_1\ a\ , S_2(a),...,S_n(a)\ = \left(\sum_{n=0}^{N-1} x_1(n)\xi_1^{-an}\right),$

$$\sum_{a=0}^{N-1} x_2\ n\ \xi_2^{-an},..., \sum_{n=0}^{N-1} x_n\ n\ \xi_n^{-an});$$

$$x_1\ n\ , x_2\ n\ ,..., x_n\ n\ = \left(N^{-1}\sum_{a=0}^{N-1} S_1\ a\ \xi_1^{an},...,\right.$$

$$\left. N^{-1}\sum_{a=0}^{N-1} S_2\ a\ \xi_2^{an},..., N^{-1}\sum_{a=0}^{N-1} S_n\ a\ \xi_n^{an}\right).$$

Приравнивая одноименные координаты заданных векторов, получим:

$$a\ = \sum_{n=0}^{N-1} x_1\ n\ \xi_1^{-an},$$

и $$x_1\ n\ = N^{-1}\sum_{a=0}^{N-1} S_1\ a\ \xi_1^{an}\ \bmod m_1\ ,$$

а также
$$\delta_2(a) = \sum_{n=0}^{N-1} x_2(n)\xi_2^{-an}, x_2(n) = \\ = N^{-1}\sum_{a=0}^{N-1} S_2(a)\xi_2^{an}(\bmod m_2); \qquad (3)$$

$$\delta_n(a) = \sum_{n=0}^{N-1} x_2(n)\xi_n^{-an}, x_n(n) = \\ = N^{-1}\sum_{a=0}^{N-1} S_n(a)\xi_n^{an}(\bmod m_n). \qquad (4)$$

Преобразования (3), (4) могут быть реализованы последовательно за n условных тактов либо параллельно во времени за один условный такт. В этом плане очевидны следующие преимущества от организации такого вида вычислений: значительное сокращение времени реализации совокупности (1) – (4) соотношений за счёт возможности совмещения операции вида (1) и (2) с операцией аналого-цифрового преобразования. Таким образом, возникает задача синтеза СОКИ адаптивного к $GF\ m_1\ + GF\ m_2\ + ... + GF\ m_n$ – арифметики.

Теоретически возможность создания такого адаптивного СОКИ обусловлена следствием следующей теоремы [2]. Пусть Z_M – кольцо классов вычетов по модулю $M = m_1^{\alpha_1} m_2^{\alpha_2} ... m_n^{\alpha_n}$ (m_i – простое число; $i = \overline{1,n}$). Тогда Z_M – изоморфно кольцу $Zm_1^{\alpha_1} + Zm_2^{\alpha_2} + ... + Zm_n^{\alpha_n}$. Элементы этого кольца – n-мерные векторы, арифметические операции над которыми осуществляются покомпонентно. Покажем это.

Пусть отображение $f : Z_M \to Z_1^{\alpha_1} + Zm_2^{\alpha_2} + ... + Zm_2^{\alpha_n}$ определено следующим образом:

$$f(a) = (a_1(\bmod m_1^{\alpha_1}), a_2(\bmod m_2^{\alpha_2}), ..., a_n(\bmod m_n^{\alpha_n})) . (5)$$

Аргумент a последовательно принимает значение от 0 до $M-1$, при этом, аргумент a_1 принимает значение от 0 до $m_1^{\alpha_1} - 1$, а аргумент a_2 принимает значение от 0 до $m_2^{\alpha_1} - 1$ и т.д. Так как m_i – простые числа, то вектор (5) в диапазоне [0, M) однозначен, следовательно, отображение f есть биекция. Кроме этого, для всех $a,b \in Z_M$ выполняется следующее равенство:

$$f(a+b) = ((a+b) \bmod m_1^{\alpha_1}, (a+b) \bmod m_2^{\alpha_2}, ...,$$

$$(a+b) \bmod m_n^{\alpha_n}) = (a(\bmod m_1^{\alpha_1}), a(\bmod m_2^{\alpha_2}), ...,$$

$$..., a(\bmod m_n^{\alpha_n})) + (b(\bmod m_1^{\alpha_1}), b(\bmod m_2^{\alpha_2}, ...,$$

$$b(\bmod m_n^{\alpha_n})) = f(a) + f(b).$$

Аналогично можно показать, что $f(ab) = f(a)f(b)$.

Следовательно, при синтезе СОКИ на основе новой машинной модулярной $Zm_1^{\alpha_1} + Zm_2^{\alpha_2} + ... + Zm_n^{\alpha_n}$ – арифметики можно получить качественно новые научные и практические результаты в плане улучшения основных тактично-технических характеристик систем обработки информации (производительности, отказоустойчивости, надежности, живучести, достоверности, а также массогабаритных и энергетических характеристик и т.п.) за счет возможности организации принципиально новой структуры СОКИ реального времени и применения новых оригинальных методов и алгоритмов обработки информации, а также реализации технических решений отдельных блоков и узлов СОКИ. Для эффективной реализации математических моделей ЦОС посредством новой $\sum_{i=1}^{n} Zm_i^{\alpha_i}$ – арифметики, определенной над конечными полями и кольцами, необходимо, чтобы посредством СОКИ можно было бы эффективно реализовать арифметические операции заданных алгебраических структур.

Реализация арифметических операций конечного поля Галуа $GF(M)$ сводится к реализации модульных операций параллельно над каждым из n конечных полей $GF(m_i^{\alpha_i})$, $i=\overline{1,n}$. В этом аспекте известный математический аппарат теории чисел, служащий основой для создания кодов в СОК, будет "адаптивен" (приспособлен) к классу целочисленных задач СОИ реального времени.

Действительно, пусть для $\chi-$ преобразований, определенных над конечным полем или кольцом, необходимо получить нужный порядок первообразного элемента. Для этого необходимо выбрать соответствующее конечное поле или кольцо, т.е. выбрать соответствующее значение модуля M. При этом M должно быть либо простым, либо разлагаться на простые сомножители.

Пусть $M=\prod_{i=1}^{n} m_i, HOD(m_i,m_j)=1$ для $i\neq j, \alpha_i=1 (i=\overline{1,n})$, тогда вычисления по модулю M, т.е. в поле $GF(M)$, заменяются параллельными вычислениями одновременно по n основаниям (модулям) m_i, т.е. параллельно в n полях Галуа $\sum_{i=1}^{n} GF(m_i)$. В этом случае СОКИ должно весьма эффективно реализовать целочисленные модульные операции над $\sum_{i=1}^{n} GF(m_i)$ – арифметикой, а это возможно только при применении МСС.

Цель статьи – показать возможность использования МСС для построения систем обработки криптографической информации, функционирующих в реальном времени шифрации.

Основные материалы исследований

Предварительные исследования показали, что использование кодов МСС дает возможность эффективно реализовать математические модели СОКИ, определенные над конечными полями или кольцами в вещественной области. В случае если $M-$ простое число, то набор m_i оснований МА должен обеспечить выполнение следующего требования $M\le\prod_{i=1}^{n} m_i$.

Рассмотрим пример реализации СОКИ задач ЦОС, в частности, задачи определения свертки цифровых сигналов $x_1(n'), x_2(n')$ посредством применения преобразований Фурье-Галуа, определенных над прямыми суммами полей Галуа $\sum_{i=1}^{n} GF(m_i)$ на основе использования СОК, заданной набором оснований $\{m_i\}$. В этом случае значения соответствующих сигналов $x_1(n'), x_2(n')$ представляются в виде остатков от последовательного деления их на набор взаимно попарно простых чисел m_i, т.е.

$$x_1(n')=(x_{11}(n') \bmod m_1, x_{12}(n') \bmod m_2,...), \quad (6)$$

и $$x_1(n')=(x_{21}(n') \bmod m_1, x_{21}(n') \bmod m_2,...),. \quad (7)$$

В соответствии с алгоритмами реализации арифметических операций в МСС соответствующие компоненты $x_{1i}(n') \bmod m_i$ и $x_{2i}(n') \bmod m_i$ векторов (6) и (7) обрабатывается в канале по модулю m_i СОКИ независимо от других компонент и параллельно во времени. В этом случае разрядность $r_{mi}=\log_2(m_i-1)+1$ канала обработки информации по основанию m_i СОКИ будет меньше разрядности $r_M=\log_2(M-1)+1$ СОКИ, обрабатывающего информацию в конечном поле Галуа $GF(M)$ по модулю $M=\prod_{i=1}^{n} m_i$. Очевидно, что совокупность остатков $x_{1i}(n') \bmod m_i$ по модулю m_i образует конечное поле Галуа $GF(m_i)$, а совокупность остатков по каждому из n полей для $i=\overline{1,n}$ можно отождествить с прямой суммой полей Галуа $\sum_{i=1}^{n} GF(m_i)$. При этом нет необходимости преобразовать результат модульной операции в исходное поле Галуа $GF(M)$.

Рассмотренный метод реализации арифметических операций в поле $GF(M)$ посредством реализации этих операций одновременно в n полях Галуа $GF(m_i)$ для $i=\overline{1,n}$ нетрудно распространить и на гиперкомплексную числовую область, в частности, простое поле Галуа $GF(M)$ может быть расширено до конечного поля комплексных чисел $Z\,i$. Воспользуемся результатами "китайской" теоремы об остатках для определения $\chi-$ преобразований над прямой суммой комплексных полей $GF(m_i^{(2)})$ [1, 4].

Отметим. что для любых взаимно простых дивизоров (идеалов) $A_i (i=\overline{1,n})$ и для любых элементов α_i кольца J существует такой элемент $\beta\in J$, что

$$\beta=\alpha_1(\bmod A_1); \beta=\alpha_2(\bmod A_2);...,\beta=\alpha_n(\bmod A_n).$$

Пусть Z_M- кольцо классов вычетов по модулю $M=\prod_{i=1}^{n} m_i$ (m_i- простое число) и пусть $Z_M\,i-$ конечное поле комплексных чисел по модулю простого числа M, тогда справедливо следу-

ющее утверждение. Кольцо, Z_M i изоморфно прямой сумме комплексных полей Галуа $\sum_{i=1}^{n} GF(m_i^{\,2})$, т.е.

$$Z_M \text{ i} \approx GF(m_1^{(2)}) + GF(m_2^{(2)}) + ... + GF(m_n^{(n)}),$$

при условии, если полином x^2+1 является неприводимым над каждым из полей $GF\ m_i^{\,2}$. Покажем это. Пусть комплексное число $A = \alpha_1 + i\alpha_2 \in Z_M$ i .. Определим следующее отображение:

$$f : \alpha_1 + \alpha_2 \to ((\alpha_{11} + \alpha_{21}) \bmod m_1, ..., (\alpha_n + \alpha_n) \bmod m_n).$$

Так как полином x^2+1 неприводим над каждым из n показателей $GF\ m_i^{\,2}$, то произвольный остаток $\alpha_{1j} + i\alpha_{2j} \bmod m_j$ принадлежит полю $GF\ m_i^{\,2}$ для всех $j = \overline{1,n}$. Таким образом, f является отображением кольца Z_M i в прямую сумму полей $GF\ m_i^{\,2}$, т.е.

$$f : Z_M \text{ i} \to GF(m_1^{(2)}) + GF(m_2^{(2)}) + ... + GF(m_n^{(2)}).$$

Пусть $A = \alpha_1 + i\alpha_2, B = \beta_1 + i\beta_2 \in Z_M$ i , тогда

$$\begin{aligned} f(A+B) &= f((\alpha_1+\beta_1) + i(\alpha_2+\beta_2)) = \\ &= (\alpha_1+\beta_1) + i(\alpha_2+\beta_2) \bmod m_1 \\ &\quad (\alpha_1+\beta_1) + (\alpha_2+\beta_2) \bmod m_2, ..., \\ &\quad (\alpha_1+\beta_1) + i(\alpha_2+\beta_2) \bmod m_1, ..., \\ &\quad (\alpha_1+\beta_1) + i(\alpha_2+\beta_2) \bmod m_n) = \\ &= ((\alpha_1+i\alpha_2) \bmod m_1 + (\beta_1+i\beta_2) \bmod m_1), \\ &\quad (\alpha_1+i\alpha_2) \bmod m_2 + (\beta_1+i\beta_2) \bmod m_2), ..., \\ &\quad (\alpha_1+i\alpha_2) \bmod m_i + (\beta_1+i\beta_2) \bmod m_i), ..., \\ &\quad (\alpha_1+i\alpha_2) \bmod m_n + (\beta_1+i\beta_2) \bmod m_n) = \\ &= [((\alpha_1+i\alpha_2) \bmod m_1 + (\alpha_1+i\alpha_2) \bmod m_2), ..., \\ &\quad (\alpha_1+i\alpha_2) \bmod m_i, ..., (\alpha_1+i\alpha_2) \bmod m_n + \\ &\quad + (\beta_1+i\beta_2) \bmod m_1, (\beta_1+i\beta_2) \bmod m_2, ..., \\ &\quad (\beta_1+i\beta_2) \bmod m_i, ..., (\beta_1+i\beta_2) \bmod m_n)] = f(A) + f(B). \end{aligned}$$

Нетрудно показать, что $f(AB) = f(A) \cdot f(B)$, т.е. заданное отображение f является гомоморфным. В [4] показано, что если ограничить отображение f только на одну из частей (реальную или мнимую) комплексного числа, то оно перейдет в изоморфизм, связывающий класс вычетов Z_M и прямую сумму $GF(m_1) + GF(m_2), +...+ ,GF(m_i), +...+ ,GF(m_n)$. Данный факт свидетельствует о том, что данное отображение f является изоморфизмом. Это подтверждает вывод об эффективности применения модулярной $\sum_{i=1}^{n} GF(m_i) -$ арифметики (использования МСС) в комплексной области.

По аналогии с $\chi -$ преобразованиями [1], определенными над конечным полем комплексных чисел, определяются преобразования над алгебраическими структурами более высоких порядков (гиперкомплексные числовые системы), в частности, над конечным кольцом кватернионов $Z_M^{(K)}$. Преимущества такого подхода состоят, в первую очередь, в отсутствии шума округления и в сохранении ассоциативного и коммутативного законов при выполнении модульных операций, что позволяет весьма действенно использовать математический аппарат МА. Данное обстоятельство обеспечивает возможность эффективной реализации СОКИ в МСС посредством алгебраической числовой структуры заданного порядка. Построение СОКИ, определенных над конечными полями и кольцами, произвольной размерности является новым, перспективным направлением в теории обработки цифровых сигналов. Однако без средств эффективной реализации таких ММ ЦОС не удается полностью использовать преимущества такого подхода. Требования реализации арифметических операций в конечных полях Галуа GF(M), в конечных полях целых комплексных чисел $Z_M^{(C)}$, а также в конечных кольцах различных структур (например, $Z_M, Z_M^{(C)}$ и т.п.) сводятся к возможности эффективной реализации модульных арифметических операций. Вследствие этого очевидно, что основой операционного устройства (ОУ) СОКИ в МСС будет являться канал обработки информации по модулю m_i, а ОУ будет представлять собой совокупность из n каналов обработки информации по соответствующим модулям m_i для $i = \overline{1,n}$, реализующую алгоритмы ЦОС посредством модулярной $GF(m_i) + GF(m_2) + ... + GF(m_n) -$ арифметики. При этом структура СОКИ полностью соответствует принципу образования кода в МСС, т.е. структура как ОУ, так и СОКИ, будет реализована, исходя из основных свойств системы остаточных классов [5, 6]. Этим и определяется высокая степень адаптации структуры СОКИ в МСС к классу решаемых криптографических задач. Кроме этого, кодам МСС присущи особенности, выявленные для рассматриваемых математических моделей систем: кодирование элементов рассмотренных алгебраических структур (вычетов по произвольному модулю m_i МСС) осуществляется в целых неотрицательных числах $(0,1,2,\ldots, m_i - 1)$, а также отсутствие привычного физического смысла результатов вычислений в конечных полях и кольцах (невозможность оперативной оценки величины операнда в МСС по его аналитическому представлению).

Выводы

Использование свойств кодов МСС позволяет создать систему обработки криптографической информации, удовлетворяющую основным требованиям по эффективной реализации абстрактных моделей систем, определенных в конечных полях и кольцах. Высокая адаптивность структуры СОКИ в МСС к моделям таких систем позволит получить качественно новые результаты, имеющие важное теоретическое и практическое значение для решения проблемы ускорения выполнения арифметических модульных операций на гиперэллиптических кривых третьего рода.

Список литературы

1. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. радио, 1968. – 440 с.

2. Виноградов И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1981. – 175 с.

3. Акушский И.Я. Основы машинной арифметики комплексных чисел / И.Я. Акушский, В.М. Амербаев, И.Т. Пак. – Алма-Ата: Наука, 1970. – 248 с.

4. Кантор И.Л. Гиперкомплексные числа / И.Л. Кантор, А.С. Солодовников. – М.: Наука, 1973. – 144 с.

5. Сиора А.А. Отказоустойчивые системы с версионно-информационной избыточностью в АСУ ТП: Монография / А.А. Сиора, В.А. Краснобаев, В.С. Харченко. – Х.: МОН, НАКУ им. Н.Е. Жуковского «ХАИ», 2009. – 320 с.

6. Барсов В.И. Методология параллельной обработки информации в модулярной системе счисления: Монография / В.И. Барсов, Л.С. Сорока, В.А. Краснобаев. – Х.: МОН, УИПА, 2009. – 268 с.

Поступила в редколлегию 20.08.2009

Рецензент: д-р техн. наук, проф. И.А. Фурман, Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Харьков.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ЗАСТОСУВАННЯ КОДІВ МОДУЛЯРНОЇ СИСТЕМИ ЧИСЛЕННЯ ДЛЯ СТВОРЕННЯ СИСТЕМИ ОБРОБКИ КРИПТОГРАФІЧНОЇ ІНФОРМАЦІЇ РЕАЛЬНОГО ЧАСУ

С.О. Мартиненко, В.А. Краснобаєв

У статті проводяться теоретичні дослідження можливості ефективного застосування модулярної системи числення для обробки криптографічної інформації над кінцевим полем в реальному часі. Результати проведених досліджень рекомендовано для обробки криптоперетворень, що базуються на арифметиці у групі точок еліптичних кривих.

***Ключові слова**: система обробки криптографічної інформації, модулярна система числення, цифрова обробка сигналів, поля Галуа, арифметичні операції по модулю.*

RESEARCH OF POSSIBILITY OF APPLICATION OF KODAS MODULYARNOY OF NUMBER FOR CREATION OF SYSTEM OF TREATMENT OF CRYPTOGRAPHIC INFORMATION OF THE REAL TIME SYSTEM

S.O. Martynenko, V.A. Krasnobaev

In the article theoretical researches of possibility of effective application of the modular number for treatment of cryptographic information system are conducted above the eventual field in real time. The results of the conducted researches are recommended for treatment of cryptotransformations, based on arithmetic in the group of points of elliptic curves.

***Keywords:** system of treatment of cryptographic information, modular number system, digital treatment of signals, fields of Galois, arithmetic operations on the module.*