УДК 681.391.837: 681.327.22

В.М. ИЛЮШКО[1], В.А. КРАСНОБАЕВ[2], Н.С. ДЕРЕНЬКО[1], Я.В. ИЛЮШКО[1], KHERY ALI ABDULLAH[1]

[1]*Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина*
[2]*Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Украина*

МЕТОДЫ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ КОДОВ МОДУЛЯРНОЙ АРИФМЕТИКИ

В данной статье предложены два метода реализации криптографических преобразований с открытым ключом на основе использования кодов модулярной арифметики (МА). Первый метод основан на использовании табличного принципа реализации арифметических операций в МА, а второй – на основе принципа кольцевого сдвига. Использование данных методов позволяет существенно повысить производительность реализации процесса криптографических преобразований.

система обработки информации, криптографические преобразования, система счисления в остаточных классах, модулярная арифметика

Введение

Актуальность темы статьи. Все современные криптопреобразования с открытым ключом, как правило, основываются на преобразованиях на алгебраических кривых (эллиптические кривые (ЭК), гиперэллиптические кривые (ГЭК), кривые Пикарда (КП) и суперэллиптические кривые (СУ)). Развитие криптографических методов направлено, в том числе, на увеличения длины ключей, что в свою очередь приводит к снижению быстродействия (пользовательской производительности) криптографических преобразований вообще и с открытым ключом в частности. Это особенно критично для обеспечения заданного уровня стойкости при реализации криптопреобразований на ЭК в системах и устройствах обработки информации специального назначения, где есть существенные ограничения по объему памяти, массе, габаритам и другим характеристикам, т.е. в тех случаях, где нет возможности использовать мощные высокопроизводительные стационарные ЭВМ с большой разрядной сеткой. Данное обстоятельство обуславливает важность и актуальность поиска методов повышения производительности криптопреобразований.

Анализ существующих литературных источников. Анализ существующих и возможных перспективных методов повышения производительности СУ в якобиане ГЭК позволил теоретически обосновать и практически показать зависимость производительности выполняемых операций СУ в якобиане ГЭК от совокупности следующих основных характеристик: – от вида реализации криптопреобразований (программная, аппаратная и программно-аппаратная); – от вида алгоритма СУ дивизоров; – от заданного базового поля, над которым задается данная кривая; – от типа кривой; – от значений коэффициентов кривой; – от выбранной системы координат, в которой представлены дивизоры якобиана ГЭК (аффинная, проективная, взвешенная и смешанная); – от принятого метода арифметических преобразований в якобиане и пр. Известные методы реализации алгоритмов СУ (метод сложения дивизоров Кантора, метод Коблица, методы арифметических преобразований дивизоров в якобиане

ГЭК второго, третьего и четвертого рода, методы сложения дивизоров различного веса, метод Карацубы для умножения и приведения по модулю в поле полиноминальных функций, метод, основанный на некоторых результатах "Китайской теоремы об остатках" и пр.) не всегда удовлетворяют требованиям по производительности процесса криптопреобразований. В то же время, в литературе [1 – 3] показана высокая эффективность применения кодов модулярной арифметики (МА), т.е. системы счисления в остаточных классах (СОК), при решении отдельных задач обработки цифровой информации (решение задач фильтрации, задач реализации БПФ и ДПФ, задач теоретико-числовых преобразований, реализация целочисленных арифметических операций конечного поля Галуа, конечного поля комплексных чисел с целыми вещественной и мнимой частями, конечных колец и пр.) с точки зрения высокой производительности их реализации. Так, известно, что преобразование Фурье связано с вычисление полинома вида $P(x)=\sum_{i=1}^{n-1}\alpha_i x^i$. Одно из приложений преобразования Фурье – вычисление свертки $\sum_{i=1}^{n}\alpha_i\beta_i$ двух n-мерных векторов

$$A=(\alpha_1,\alpha_2,...,\alpha_n) \text{ и } B=(\beta_1,\beta_2,...,\beta_n).$$

В данном случае операция свертки является полным аналогом реализации арифметических операций умножения двух чисел A и B в МА с последующим сложением компонент типа

$$\alpha_i\beta_i(\text{mod } m_i)+\alpha_j\beta_j(\text{mod } m_j).$$

Данное обстоятельство обуславливает важность и актуальность поиска методов повышения производительности криптопреобразований на основе использования свойств непозиционных кодовых структур МА. Применение данных методов позволяет существенно повысить пользовательскую производительность обработки криптографической информации.

Цель данной статьи – разработка методов высокопроизводительной реализации криптографических преобразований с открытым ключом на основе использования свойств непозиционных кодовых структур модулярной арифметики.

Основная часть

В литературе [1, 3] детально рассмотрено влияние основных свойств (независимость, равноправность и малоразрядность остатков, представляющих операнд) МА на структуру и принципы функционирования системы обработки криптографической информации (СОИ) в МА. В частности, показано, что малоразрядность остатков в представлении чисел в модулярной арифметике дает возможность широкого выбора вариантов теоретических и системотехнических решений при реализации модульных арифметических операций.

Известно, что существует четыре принципа реализации арифметических операций в МА: сумматорный принцип (СП) (на базе малоразрядных двоичных сумматоров [1]); табличный принцип (ТП) (путем использования ПЗУ, созданных на основе систолических и программируемых логических матриц (ПЛМ), СБИС, а также ПЛИС [1, 3]); прямой логический принцип (ПЛП) реализации арифметических операций, основанный на описании модульных операций на уровне систем переключательных функций, посредством которых формируются значения двоичных разрядов результирующих вычетов (в качестве элементной базы для технической реализации данного принципа целесообразно использовать ПЛИС [3]); принцип кольцевого сдвига (ПКС), основанный на использовании кольцевых регистров сдвига (КРС) [4, 5].

Отсутствие межразрядных связей (отсутствие процесса переносов) между остатками числа в СОК (между двоичными разрядами внутри остатков при СП, ПЛП и, в меньшей степени, при ПКС межраз-

рядная логическая и физическая связь существует) в обрабатываемых в СОИ операндах в процессе криптопреобразований (при реализации модульных операций), на основе ТП и ПКС, является одной из главных и наиболее привлекательных особенностей модулярной арифметики. В позиционной системе счисления (ПСС) выполнение арифметической операции предполагает последовательную обработку разрядов операндов по правилам, определяемым содержанием данной операции, и не может быть закончено до тех пор, пока не будут последовательно определены значения всех промежуточных результатов с учетом всех связей между разрядами.

Таким образом, ПСС, в которых представляется и обрабатывается информация в современных СОИ, обладают существенным недостатком – наличием межразрядных связей, которые накладывают свой отпечаток на методы реализации арифметических операций, усложняют аппаратуру, снижают достоверность вычислений и ограничивают быстродействие реализации криптографических преобразований. Поэтому естественно изыскание возможностей построения такой арифметики, в которой бы поразрядные связи отсутствовали. В этом плане обращает на себя внимание система счисления в остаточных классах. Система остаточных классов обладает ценным свойством независимости друг от друга остатков по принятой системе оснований. Эта независимость открывает широкие возможности в построении не только новой машинной арифметики, но и принципиально новой схемной реализации СОИ, которая, в свою очередь, заметно расширяет применение машинной арифметики. Во многих литературных источниках отмечается, что одним из практических направлений повышения пользовательской производительности вычислительных средств является внедрение нетрадиционных методов представления и параллельной обработки информации в числовых системах с параллельной структурой, и в частности, в так называемых модулярных системах счисления, обладающих максимальным уровнем внутреннего параллелизма в организации процесса переработки информации. К модулярным системам счисления относится и непозиционная система счисления в остаточных классах.

Как ранее отмечалось, одно из свойств МА – малоразрядность остатков, представляющих операнд. Именно это свойство позволяет существенно повысить быстродействие выполнения арифметических операций за счет возможности применения (в отличии от ПСС) табличной арифметики, где арифметические операции сложения, вычитания и умножения выполняются практически в один такт.

Поиск путей одновременного повышения производительности обработки информации и надежности функционирования СОИ привел к необходимости разработки методов реализации модульных операций, основанных на использовании ТП и ПКС.

В общем случае матричное (табличное) операционное устройство СОИ для реализации арифметических операций (которые реализуется в унитарном коде) представляет собой двухвходовое ПЗУ. Для каждого из входов количество входных шин для l-байтовой ($8l$ двоичных разряда) СОИ равно 2^{8l}. При этом общее количество логических схем совпадение "И" в узлах ПЗУ (которое, в основном, и определяет общее количество оборудования табличного операционного устройства СОИ) равно

$$N_l = 2^{8l} \times 2^{8l} = 2^{16l}. \qquad (1)$$

Исходя из формулы (1) очевидно, что табличная реализация целочисленных модульных арифметических операций в ПСС целесообразна только для значения $l = 1$. Действительно, в этом случае $N_1 = 2^{16} = 65536$, что является приемлемым количеством оборудования для современного развития элементной базы. Однако, как отмечалось выше, тенденция в реализации криптографических преобразований направлена на увеличение длины разрядной сетки СОИ. Уже сейчас предлагается к практическому использованию СОИ для криптографических преоб-

разований с $l = 4$ и $l = 8$. В этом случае $N_4 = 2^{32} \times 2^{32} = 2^{64}$ и $N_8 = 2^{64} \times 2^{64} = 2^{128}$. Если учесть, например, что $2^{32} = 4294967296$, $2^{64} = 18446744073709551616$, а $2^{128} \approx 3{,}4 \times 10^{38}$, то очевидно, что табличные методы реализации арифметических операций в ПСС практически не применимы.

Иные, положительные, результаты можно получить, если рассмотреть реализацию криптографических преобразований в МА. Действительно, при реализации криптопреобразований для СОИ в МА с $l = 4$ и $l = 8$ соответственно имеем $N_{4\,МА} = 2397$ и $N_{8\,МА} = 13275$ (в общем случае, для матричного операционного устройства СОИ $N_{l\,MA} = \sum_{i=1}^{n} m_i^2$), что вполне приемлемо при реализации арифметических операций сложения, вычитания и умножения в МА, используя современную элементную микроэлектронную базу (СБИС, ПЛМ или ПЛИС).

Вышеизложенное подтверждает целесообразность и эффективность практического использования только МА для реализации криптографических алгоритмов (реализующих в конечном итоге совокупность целочисленных модульных операций сложение и умножение) табличными методами.

Табличный метод реализации операции модульного умножения в МА реализуется посредством использованием кода табличного умножения (КТУ). В этом случае таблица $\alpha_i\beta_i \pmod{m_i}$ модульного умножения для произвольного основания m_i СОК симметрична относительно левой (главной) и правой диагоналей, а также вертикали и горизонтали. Симметричность относительно левой диагонали определяется коммутативностью операции $\alpha_i\beta_i$ умножения, а симметричность относительно правой диагонали определяется выполнением следующего сравнения

$$(m_i - \alpha_i)(m_i - \beta_i) \equiv \alpha_i\beta_i (\mathrm{mod}\ m_i).$$

Симметричность относительно вертикали и горизонтали определяется из условия кратности значения модуля сумме симметричных чисел таблицы умножения

$$\alpha_i\beta_i + \alpha_i(m_i - \beta_i) \equiv 0 (\mathrm{mod}\ m_i),$$

$$\alpha_i\beta_i + \beta_i (m_i - \alpha_i) \equiv 0 (\mathrm{mod}\ m_i).$$

В этом случае очевидно, что для табличной реализации операции модульного умножения $\alpha_i\beta_i \pmod{m_i}$ достаточно иметь числовую информацию только о ее восьмой части.

Отсюда возникает возможность упростить таблицу модульного умножения.

Для реализации операции $\alpha_i\beta_i \pmod{m_i}$ применяются методы специального кодирования, позволяющие в четыре раза уменьшить таблицу модульного умножения. Решение поставленной задачи возможно в результате применения специальных кодов. Рассмотрим один из вариантов выполнения операции модульного умножения посредством использования КТУ (табл. 1, 2 для $m_i = 5$).

Входные числа α_i и β_i, лежащие в диапазоне $[0, (m_i - 1)/2)$, могут быть закодированы произвольным способом, а значения $\alpha_i(\beta_i)$, лежащие в диапазоне $[(m_i + 1)/2, m_i - 1)$, кодируются как $m_i - \alpha$ $(m_i - \beta_i)$. Для отличия диапазонов вводится следующий индекс (признак) КТУ:

$$\gamma_a(\gamma_\beta) = \begin{cases} 0, \text{при } 0 \le \alpha_i(\beta_i) \le (m_i - 1)/2; \\ 1, \text{при } (m_i + 1)/2 \le \alpha_i(\beta_i) \le m_i - 1. \end{cases}$$

Алгоритм определения результата операции модульного умножения $\alpha_i'\beta_i' (\mathrm{mod}\, m_i)$ в СОК посредством использования КТУ следующий: если заданы два операнда в КТУ

$$\alpha_i = (\gamma_\alpha, \alpha_i'), \quad \beta_i = (\gamma_\beta, \beta_i'),$$

то для того, чтобы получить произведение этих чисел по модулю m_i, достаточно найти произведение $\alpha_i'\beta_i' (\mathrm{mod}\, m_i)$ и инвертировать его обобщенный индекс γ_i в случае, если γ_α отлично от γ_β, т.е.

$$\alpha_i\beta_i (\mathrm{mod}\ m_i) = (\gamma_i, \alpha_i'\beta_i' (\mathrm{mod}\ m_i)),$$

где:

$$\gamma = \begin{cases} \overline{\gamma}_i, \text{ при } \gamma_\alpha \neq \gamma_\beta; \\ \gamma_i, \text{ при } \gamma_\alpha = \gamma_\beta, \end{cases}$$

$$\alpha_i' = \begin{cases} \alpha_i, \text{ при } \gamma_\alpha = 0; \\ m_i - \alpha_i, \text{ при } \gamma_\alpha = 1. \end{cases}$$

Таблица 1

Код табличного умножения

α_i	КТУ		α_i	КТУ	
	γ_α	α_i'		γ_α	α_i'
1	0	1	3	1	2
2	0	2	4	1	1

Таблица 2

Таблица модульного умножения

β_i \ α_i	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Эффективная табличная реализация модульных арифметических операций сложения и вычитания с использованием КТУ в литературе либо практически не рассматривалась, либо такая реализация считалась большинством исследователей теоретически и практически невозможной.

Основная трудность заключается в том, что довольно сложно синтезировать табличные алгоритмы выполнения этих модульных операций, так как таблицы реализации модульных операций сложения и вычитания различны по своей цифровой структуре, вследствие чего они не обладают теми свойствами симметрии, которыми обладают таблицы модульного умножения.

Однако совершенно иные результаты можно получить, исследуя возможности реализации одной модульной операции с помощью таблицы, реализующей операцию, ей обратную, и наоборот.

При исследовании цифровых свойств таблиц модульных операций сложения и вычитания доказано следующее аналитическое соотношение

$$\left[(\gamma_\alpha, \alpha_i') + (\gamma_\beta, \beta_i')\right] + \left\{\left[m_i - (\gamma_\alpha, \alpha_i')\right] - (\gamma_\beta, \beta_i')\right\} = 0 \pmod{m_i}, \quad (2)$$

где $\alpha_i = (\gamma_\alpha, \alpha_i')$, $\beta_i = (\gamma_\beta, \beta_i')$ – входные операнды, представленные в КТУ. Запишем выражение (2) в виде

$$(\gamma_\alpha, \alpha_i') + (\gamma_\beta, \beta_i') = m_i - \left\{\left[m_i - (\gamma_\alpha, \alpha_i')\right] - (\gamma_\beta, \beta_i')\right\}. \quad (3)$$

Из выражения (3) следует, что для получения результата операции модульного сложения в КТУ достаточно знать результат операции модульного вычитания, т.е. возникает возможность эффективно (с точки зрения уменьшения количества оборудования ПЗУ) использовать КТУ одновременно для трех модульных арифметических операций: умножения, сложения и вычитания.

На основании выражения (3) рассмотрим метод, посредством которого можно будет осуществлять выполнения любой из трех арифметических операций в СОК: умножение, сложение и вычитание. Операция модульного сложения осуществляется посредством алгоритма, описанного выражением (3). Составим алгоритм выполнения операции модульного сложения с помощью таблицы, для выполнения операции модульного вычитания $(\alpha_i' - \beta_i') \bmod m_i$.

В соответствии с выражением (3) рассмотрим алгоритм реализации операции модульного сложения.

1. Уменьшаемое $\alpha_i = (\gamma_\alpha, \alpha_i')$ инвертируется по модулю m_i, т.е. получим следующее выражение: $\overline{\alpha}_i = \left((\gamma_\alpha + 1) \bmod 2, \alpha_i'\right)$. Вычитаемое (γ_β, β_i') оставляем без изменений.

2. Посредством ПЗУ, реализующего операцию модульного вычитания, по входным операндам α_i' и β_i' определяется результат операции

$(\alpha_i' - \beta_i') \bmod m_i$. Как и для алгоритма модульного умножения, индекс γ_i результата операции модульного вычитания формируется в соответствии со значениями индексов соответствующих операндов, т.е. в соответствии со значениями $(\gamma_\alpha + 1) \bmod 2$ и γ_β, где:

$$\gamma_i = \begin{cases} \overline{\gamma}, \text{ если } (\gamma_\alpha + 1) \bmod 2 \neq \gamma_\beta; \\ \gamma, \text{ если } (\gamma_\alpha + 1) \bmod 2 = \gamma_\beta. \end{cases}$$

Следовательно, результат операции модульного вычитания будет иметь следующий вид:

$$(\gamma_i, (\alpha_i' - \beta_i') \bmod m_i).$$

3. Полученный результат модульного вычитания инвертируем по модулю m_i, т.е.

$$((\gamma_i + 1) \bmod 2, (\alpha_i' - \beta_i') \bmod m_i).$$

Несмотря на различие цифровой структуры таблиц модульных операций сложения, вычитания и умножения, создан новый оригинальный табличный метод реализации арифметических операций в МА. На основании данного метода можно синтезировать конструктивно простую, высоконадежную и сверхпроизводительную СОИ в МА, основу которого составляют три отдельных коммутатора (табл. 2, 3 и 4), каждый из которых реализует только 0,25 части соответствующей полной таблицы модульных операций умножения (табл. 2) и вычитания (табл. 4) (первый коммутатор – II квадрант таблицы умножения); второй и третий коммутаторы – соответственно I и II квадранты таблицы 4 вычитания).

Таблица 3

Таблица модульного сложения

β_i \ α_i	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

В этом плане код табличного умножения приобрел новое качество и стал универсальным табличным кодом для выполнения трех вышеприведенных арифметических операций в МА.

Таблица 4

Таблица модульного вычитания

β_i \ α_i	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

При табличном варианте реализации арифметических операций отсутствуют межразрядные связи между обрабатываемыми операндами вообще, однако для достаточно большой разрядной сетки СОИ (для больших по величине модулей СОК) резко увеличивается количество и сложность оборудования операционного устройства. Важно и актуально рассмотреть промежуточный вариант реализации арифметических операций в МА, основанный на применении принципа кольцевого сдвига.

В [4, 5] предложен принцип реализации арифметических операций в МА – принцип кольцевого сдвига, особенность которого заключается в том, что результат арифметической операции $(\alpha_i \pm \beta_i) \bmod m_i$ по произвольному модулю СОК, заданной совокупностью $\{m_j\}$ $(j = \overline{1,n})$ оснований, определяется только за счет циклических сдвигов заданной цифровой структуры. Действительно, известная теорема Кэли устанавливает изоморфизм между элементами конечной абелевой группы и элементами группы перестановок. В этом случае матрица сложения для произвольного m_i модуля СОК будет задана табл. 5.

Одним из следствий теоремы Кэли является вывод о том, что отображение элементов абелевой группы на группу всех целых чисел является гомоморфным. Это обстоятельство позволяет организовать процесс определения результата арифметиче-

ских операций в МА посредством использования ПКС.

Таблица 5

Таблица Кэли для произвольного значения m_i

β_i	α_i				
	0	1	2	...	m_i-1
0	0	1	2	...	m_i-1
1	1	2	3	...	0
2	2	3	4	...	1
...	...	...	...	...	...
m_i-1	m_i-1	0	1	...	m_i-2

Так, известно, что операнд в МА представляется набором из n остатков $\{\alpha_i\}$, образованных путем последовательного деления исходного числа A на n взаимно попарно простых чисел $\{m_i\}$, для $(i=\overline{1,n})$. В этом случае совокупность остатков $\{m_i\}$ непосредственно отождествляется с суммой n простых полей Галуа вида $\sum_{i=1}^{n} GF(m_i)$.

Для рассмотрения метода реализации арифметических операций в МА достаточно рассмотреть вариант для произвольного конечного поля Галуа $GF(m_i)$ при i = const , т.е. для конкретной приведенной системы вычетов по модулю m_i.

Пусть для заданной операции модульного сложения $(\alpha_i+\beta_i)\bmod m_i$ в поле $GF(m_i)$ составлена таблица Кэли (табл. 5). Из существования нейтрального элемента в поле $GF(m_i)$ следует, что в табл. 5 есть строка (столбец), в которой элементы данного поля стоят в порядке возрастания, а из того факта, что в поле вычетов $GF(m_i)$ эти элементы различны (порядок группы равен m_i), следует, что в каждой строке (столбце) табл. 5 содержатся все элементы поля ровно по одному разу. Использование перечисленных свойств позволяет реализовать операции модульного сложения и вычитания в МА путем применения ПКС посредством n кольцевых $M=m_i([\log_2(m_i-1)]+1)$ -разрядных сдвигающих регистров.

Пусть произвольная алгебраическая система представлена в виде $S=\langle G,\odot\rangle$, где G – непустое множество; $\otimes$ – тип операции, определенной для любых двух элементов α_i, $\beta_i\in G$. Операция $\oplus$ сложения в множестве классов вычетов R, порожденных идеалом J, образует новое кольцо, называемое кольцом классов вычетов R/J. Его можно представить в виде Z/m_i, где Z – множество целых чисел 0, ±1, ±2,... (если основание СОК m_i – простое число, то Z/m_i – поле). Данное обстоятельство, как указывалось выше, и обусловливает возможность реализации арифметической операции сложения в МА без межразрядных переносов и вычислений промежуточных результатов сложения для одного двоичного разряда сумматора путем только кольцевого сдвига содержимого разрядов кольцевых сдвигающих регистров.

На основе предложенного в [4] принципа разработан метод реализации арифметических операций в МА (метод двоичного позиционно-остаточного кодирования). Суть разработанного метода состоит в том, что исходная цифровая структура для каждого модуля (основания) СОК представляется в виде содержимого первой строки (столбца) таблицы модульного сложения (вычитания) $(\alpha_i\pm\beta_i)\bmod m_i$ вида

$$P_0^{(m_i)}=\left[P_0(\alpha_0)\Big\|P_1(\alpha_1)\Big\|...\Big\|P_{m_i-1}(\alpha_{m_i-1})\right], \quad (4)$$

где $\|$ – операция конкатенации (склеивания);

$P_v(\alpha_v)$ – k-разрядный двоичный код; соответствующий значению α_v-го остатка $(\alpha_v=\overline{0,m_i-1})$ числа по модулю m_i ; ($k=\lceil\log_2(m_i-1)+1\rceil$).

Таким образом, посредством используемых в ПСС кольцевых регистров сдвига легко реализовать арифметические операции в МА. При этом степени циклических перестановок, исходя из (4), определя-

ется следующими выражениями:

$$\left[P_0(\alpha_0)\left\|P_1(\alpha_1)\right\|...\left\|P_{m_i-1}(\alpha_{m_i-1})\right.\right]= \\ =\left[P_z(\alpha_z)\left\|P_{z+1}(\alpha_{z+1})\right\|...\left\|P_0(\alpha_0)\right\|...\right. \\ \left....\left\|P_{m_i-1}(\alpha_{m_i-1})\right.\right]^Z, \quad (5)$$

или

$$\left[P_0(\alpha_0)\left\|P_1(\alpha_1)\right\|...\left\|P_{m_i-1}(\alpha_{m_i-1})\right.\right]^{-z}= \\ =\left[P_{m_i-1-z}(\alpha_{m_i-1-z})\right\|...\left\|P_{m_i-z}(\alpha_{m_i-z1})\right\| = \\ =\left\|...\left\|P_0(\alpha_0)\right\|P_1(\alpha_1)\right\|...\left\|P_{m_i-z-2}(\alpha_{m_i-z-2})\right]. \quad (6)$$

Отметим, что

$$\left[P_0(\alpha_0)\left\|P_1(\alpha_1)\right\|...\left\|P_{m_i-1}(\alpha_{m_i-1})\right.\right]^{m_i}=\varepsilon,$$

т.е. при $z = m_i$ все элементы упорядоченного множества $\left\{P_j(\alpha_i)\right\}$ $(j=\overline{0,m_i-1})$ остаются на исходном месте. При технической реализации данного метода первый операнд α_i определяет номер α_{α_i} разряда $P_{\alpha_i}(\alpha_{\alpha_i})$, с содержимым результата модульной операции по модулю m_i, а второй операнд β_i – число разрядов КРС ($\beta_i k$ -двоичных разрядов), на которые необходимо провести сдвиги исходного (4) содержимого КРС в соответствии с алгоритмами (5), (6). Основными недостатками предложенного метода реализации арифметических операций в СОК является сравнительно большое время выполнения целочисленных арифметических модульных операций, что снижает эффективность использования ПКС. Этот недостаток обусловлен тем, что структура $P^{(m_i)}$ (см. (5)) представлена набором исходных остатков первой строки матрицы $(\alpha_i+\beta_i)\bmod m_i$, отображаемых двоичным кодом. В этом случае время реализации модульного сложения двух операндов $A=(\alpha_1,\alpha_2,...,\alpha_{n-1},\alpha_n)$ и $B=(\beta_1,\beta_2,...,\beta_{n-1},\beta_n)$ в МА определяется выражением

$$t_{сл}=k\beta_{\max\ i}\tau, \quad (7)$$

где τ – время сдвига одного двоичного разряда КРС.

Рассмотрим метод реализации арифметических операций в СОК, лишенный указанного недостатка, метод унитарного позиционно-остаточного кодирования, согласно которому информационная структура $P^{(m_i)}$ произвольного модуля m_i СОК представляется в виде унитарного (m_i-1)-разрядного кода:

$$P^{(m_i)}=\left[P(\alpha_{i-1})\left\|P(\alpha_{i-2})\right\|...\left\|P(1)\right\|P(0)\right], \quad (8)$$

где $P(\alpha_j)$ – двоичный разряд цифровой структуры (7), единичное состояние которого соответствует значению операнда a_j, представленного унитарным кодом $(\alpha_j=\overline{0,m_i-1})$. В этом случае исходное состояние КРС состоит из m_i-1 двоичных разрядов.

При этом первый операнд a_j, отображаемый унитарным кодом по произвольному модулю m_i СОК, заносится в *j*-й разряд КРС, т.е переводит *j*-й двоичный разряд в единичное состояние. Второй операнд β_i указывает на число сдвигом *z* содержимого КРС, определяя время реализации арифметических операций по модулю m_i СОК, т.е.

$$t_{сл}=\beta_i\tau. \quad (9)$$

Отметим, что время реализации арифметической операции $A + B$ в МА будет определяться временем выполнения операции для максимального значения $(\beta_{\max\ i}\ \ (i=\overline{1,n})$ остатка из совокупности $\{\beta_i\}$ для данного операнда $B=(\beta_1,\beta_2,...,\beta_n)$, т.е.

$$t_{\pm}=\beta_{\max\ i}\tau. \quad (10)$$

Анализ выражений (9) и (10) показывает, что разработанный метод унитарного позиционно-остаточного кодирования сокращает в $k=\left[\log_2(m_i-1)+1\right]$ раз время выполнения арифметических операций по сравнению с методом двоичного кодирования.

Расчет времени выполнения арифметических операций при криптографических преобразований, проведенный в [8, 9, 11], показал высокую эффек-

тивность применения метода унитарного кодирования с точки зрения времени реализации арифметических операций в СОК по сравнению с методом двоичного кодирования и временем реализации таких же операций в двоичных ПСС. Полученные результаты расчетов времени реализации арифметических операций в МА могут быть использованы при оценке и сравнительном анализе вычислительной сложности реализации алгоритмов криптопреобразований.

Выводы

В данной статье предложено два метода реализации криптографических преобразований с открытым ключом: табличный метод с использованием кода табличного умножения и метод позиционно-остаточного кодирования . Данные методы основаны на представлении и обработке целочисленной цифровой информации, представленной в модулярной арифметике. На основе данных методов разработаны алгоритмы реализации арифметических операций модульного сложения, вычитания и умножения, что является основой криптографических преобразований.

Основное преимущество первого предложенного метода, основанного на ТП, состоит в возможности достижения сверхвысокого быстродействия обработки информации.

Так, результат выполнения арифметической операции табличным методом может быть получен в момент поступления входных данных на обработку, т.е. в один такт, что недостижимо для обычных двоичных СОИ в ПСС. Таким образом, время выполнения арифметических операций в МА сравнимо с тактовой частотой СОИ, что принципиально невозможно для СОИ в ПСС.

Второй предложенный метод (метод позиционно-остаточного кодирования), основанный на ПКС, также обеспечивает высокое быстродействие (в сравнении с ПСС) реализации алгоритмов криптопреобразований, а также обеспечивает повышение достоверности вычислений, за счет использования уникальных теоретических положений принципа кольцевого сдвига, при одновременном уменьшении (в сравнении с ТП) количества оборудования СОИ.

Полученные результаты исследований, проведенных в статье, целесообразно использовать в системах и устройствах обработки больших массивов цифровой информации, представленной в целочисленном виде, в реальном времени. В частности, данные методы рекомендованы для использования в системах и устройствах обработки дискретной информации для повышения производительности реализации криптографических преобразований с открытым ключом.

Литература

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

2. Лавриненко Д.И. Применение быстрого преобразования Фурье в криптографических преобразователях // Радиотехника. Всеукр. Межвед. науч.-техн. сб., 2000. – Вып. 114. – С. 75-79.

3. Жихарев В.Я., Илюшко Я.В., Кравець Л.Г., Краснобаев В.А. Методы и средства обработки информации в непозиционной системе счисления в остаточных классах. – Житомир: Волынь, 2005. – 220 с.

4. Долгов В.И., Краснобаев В.А., Кононова И.В. Метод и алгоритмы реализации арифметических операций в системе остаточных классов // Электронное моделирование. – 1990. – №5. – С. 70-72.

5. Краснобаев В.А. Методы реализации модульных операций в системах цифровой обработки информации // Радиотехника. – 2001. – Вып. 119. – С. 130-134.

Поступила в редакцию 3.11.2006

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