PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2014, t. II, s. 371–382

http://dx.doi.org/10.16926/tiib.2014.02.32

Mikhail Selianinau
Akademia im. Jana Długosza
al. Armii Krajowej 13/15, 42-200 Częstochowa
e-mail: m.selianinov@ajd.czest.pl

KRYPTOGRAFICZNA OCHRONA DANYCH NA PODSTAWIE MINIMALNIE NADMIERNYCH WIELOMIANOWO-SKALARNYCH MODULARNYCH SYSTEMÓW LICZBOWYCH

Streszczenie. Obecnie jakość realizacji procedur przetwarzania informacji zależy w dużym stopniu od wybranego modelu matematycznego organizacji tego procesu i zrealizowanej na jego podstawie technologii informacyjnej.
Istnieje szereg naukowych i praktycznych rodzajów działalności, gdzie występuje potrzeba przetwarzania informacji przedstawionej w formie wielomianów. Działania na wielomianach odgrywają istotną rolę we współczesnej algebrze komputerowej, cyfrowym przetwarzaniu sygnałów, teorii kodowania, kryptografii itd. W związku z tym duże zainteresowanie znajduje modularna technika równoległych struktur obliczeniowych zdefiniowanych w zakresach wielomianów.
W artykule opisano algorytm kryptograficzny, który pozwala wykonywać operacje blokowego szyfrowania informacji przy użyciu minimalnie nadmiernych wielomianowo-skalarnych modularnych systemów liczbowych. W takich systemach na górnym poziomie jako podstawy wybierane są nierozkładalne wielomiany, a na dolnym poziomie wykorzystuje się minimalnie nadmierne modularne kodowanie elementów z zakresu skalarów. W tym przypadku wielomian z pozycyjnym przedstawieniem współczynników może być jednoznacznie definiowany jako zbiór reszt według wybranych modułów systemu liczbowego.
Użycie minimalnie nadmiernego kodowania pozwala istotnie zwiększyć efektywność metod i algorytmów kryptograficznych kosztem optymalizacji procedur niemodułowych.
Słowa kluczowe: bezpieczeństwo informacji, kryptosystem, kryptogram, szyfrowanie, klucz publiczny, klucz prywatny, modularna arytmetyka, wielomian, modularne systemy liczbowe.

CRYPTOGRAPHIC PROTECTION OF DATA BASED ON MINIMAL REDUNDANT POLYNOMIAL-SCALAR MODULAR NUMBER SYSTEMS

Abstract. At the present time, quality of the execution of information processing procedures is largely determined by the selected mathematical model of the organization of information processing and the information technology implemented on this basis.
There are many scientific and applied researches which demand processing the information presented in the form of polynomials. Operations over the polynomials are very important in modern computer algebra, digital signal processing, coding theory, cryptography, etc. At the same time, modular technology of parallel computing structures defined on polynomial ranges is of great interest.
This article describes the cryptographic algorithm that allows us to perform the block encryption of information using minimal redundant polynomial-scalar modular number systems. In these systems, at the upper level the normalized polynomials of the first degree are used as a basis, whereas at the lower level the elements of scalar range are represented in minimal redundant modular code. In this case a polynomial with the positional representation of the coefficients can be uniquely defined as a sequence of residues with respect to selected bases.
The efficiency of the cryptographic methods and algorithms is significantly increased due to the optimization of the non-modular procedures when using the minimal redundant coding.
Keywords: information security, cryptosystem, cryptogram, encryption, public key, private key, modular arithmetic, polynomial, modular number system.

Wstęp

Informatyzacja jest cechą charakterystyczną współczesnego życia społeczeństwa. W miarę rozwoju i komplikacji środków, metod i form przetwarzania informacji zwiększa się zależność społeczeństwa od stopnia bezpieczeństwa wykorzystywanych technologii informacyjnych, od których czasami zależy dobrobyt, a czasami i życie wielu osób. Informacja jest takim samym strategicznym zasobem, jak surowce i energia, i dlatego musi się chronić, bronić i pewnie przechowywać.

Aktualność i znaczenie problemów związanych z bezpieczeństwem informacyjnym są spowodowane następującymi przyczynami:

- radykalne zwiększenie mocy obliczeniowej współczesnych komputerów przy jednoczesnym uproszczeniu ich eksploatacji;
- gwałtowny wzrost objętości informacji, która się gromadzi, przechowuje i przetwarza za pomocą komputerów;

- ulokowanie w tych samych bazach danych informacji różnego przeznaczenia i różnej przynależności;
- wysokie tempo wzrostu liczby komputerów osobistych, które są stosowane w różnych obszarach działalności;
- drastyczne rozszerzenie kręgu użytkowników mających bezpośredni dostęp do zasobów obliczeniowych i baz danych;
- szybki rozwój narzędzi programowych, które nie spełniają nawet minimalnych wymogów bezpieczeństwa;
- rozpowszechnienie technologii sieciowych i podłączenie sieci lokalnych do sieci globalnych;
- rozwój globalnej sieci Internet, która praktycznie nie zapobiega naruszeniom bezpieczeństwa informacyjnego na całym świecie.

Bezpieczeństwo informacyjne określa zabezpieczenie informacji od przypadkowych i umyślnych działań, które mogą spowodować znaczne straty właścicieli informacji. Ważne miejsce wśród środków ochrony informacji zajmuje kryptografia. Dziś bez stosowania metod i algorytmów kryptograficznych nie jest możliwe przedstawienie oraz spełnienie takich zadań bezpieczeństwa informacji, jak poufność, całość i autentyfikacja. Podstawą realizacji tych mechanizmów ochrony informacji jest szyfrowanie danych [2, 4].

Współczesne systemy telekomunikacyjne charakteryzują się wysoką szybkością i pozwalają przekazywać dużą objętość informacji w jednostce czasu. To powiązano w pierwszej kolejności z pojawieniem się nowych technologii informacyjnych, takich jak wideo- i audiokomunikacja, poczta głosowa, wideokonferencje. Ponieważ przekazywanie informacji dźwiękowej, graficznej i wideoinformacji w wielu przypadkach wymaga poufności, to powstaje zadanie szyfrowania dużej ilości danych w czasie rzeczywistym.

Niezawodność wykorzystywanych systemów szyfrowania jest związana z długością klucza: im dłuższy jest klucz, tym bardziej bezpieczny jest kryptosystem. Obecnie możliwości realizacji sprzętowej i programowej szyfrów znacznie zwiększyły się w porównaniu z końcem XX wieku. Jednak proporcjonalnie zwiększyły się też możliwości analizy kryptograficznej. W konsekwencji tego znacznie wzrosły wymagania dotyczące odporności algorytmów kryptograficznych, które spowodowały zmiany w nowoczesnych sposobach podejścia do konstrukcji szyfrów blokowych [2, 3].

W artykule opisano algorytm kryptograficzny, który pozwala wykonywać operacje blokowego szyfrowania informacji przy użyciu minimalnie nadmiernych wielomianowo-skalarnych modularnych systemów liczbowych. W danych systemach na górnym poziomie jako podstawy wybierane są nierozkładalne wielomiany, a na dolnym poziomie wykorzystuje się minimalnie nadmierne modularne kodowanie elementów z zakresu skalarów. W tym przypadku wielomian z pozycyjnym przedstawieniem współczynników może być jednoznacz-

nie definiowany jako zbiór reszt według wybranych modułów systemu liczbowego. Użycie minimalnie nadmiernego kodowania pozwala istotnie zwiększyć efektywność metod i algorytmów kryptograficznych.

Zasady kryptograficznej ochrony informacji

Podstawą technik kryptograficznych zabezpieczenia informacji są matematyczne algorytmy szyfrowania danych w celu ich ochrony przed przeczytaniem przez nielegalnych użytkowników. Szyfrowanie, czyli sposób przekształcenia otwartej informacji do poufnej i odwrotnie, stosuje się dla przechowywania ważnej informacji w niepewnych źródłach lub przekazywania jej przez niezabezpieczone kanały komunikacji. Ten sposób ochrony informacji w żaden sposób nie kontroluje rozpowszechniania informacji i nie monitoruje płynności odbiorcy. Dlatego niezawodność środków ochrony kryptograficznej zależy od niezawodności zastosowanej metody szyfrowania a podwyższanie poziomu ochrony związane jest z podwyższeniem odporności algorytmu na ujawnienie [2-4].

Obecnie istnieje cały szereg algorytmów szyfrowania danych. Wszystkie narzędzia kryptograficznej ochrony informacji mogą być podzielone na dwie duże grupy. Podstawę pierwszej grupy stanowią metody zbudowane w oparciu na szyfrowaniu symetrycznym, którego charakterystyczną cechą jest zastosowanie tego samego klucza do szyfrowania i deszyfrowania informacji. Klucz algorytmu musi być przechowywany w tajemnicy przez obie strony. Użytkownicy wybierają algorytm szyfrowania przed początkiem wymiany wiadomości. Do drugiej grupy odnoszą się systemy kryptograficzne, które oparte są na zastosowaniu asymetrycznych algorytmów szyfrowania. Te systemy charakteryzują się tym, że wykorzystują dwa różne klucze. W takich systemach szyfrowania klucz publiczny jest transmitowany przez niezabezpieczony otwarty kanał komunikacyjny i wykorzystywany jest dla szyfrowania informacji. Do deszyfrowania wiadomości wykorzystuje się klucz prywatny, który jest znany tylko odbiorcy. Należy wskazać, że algorytmy asymetryczne są pracochłonne w porównaniu z typowymi algorytmami symetrycznymi, więc w praktyce są one zwykle stosowane w przypadkach, gdy ilość zaszyfrowanej informacji jest mała, a wiadomość jest bardzo ważna [2, 4].

Symetryczne systemy kryptograficzne w porównaniu do asymetrycznych systemów mają następujące zalety:

- szybkość szyfrowania i deszyfrowania,
- łatwość realizacji,
- znacznie mniejsze wymagane zasoby obliczeniowe,
- mniejsza konieczna długość klucza,
- doskonale zbadane algorytmy.

Należy jednak również zwrócić uwagę na następujące wady:

- wymaganie dość dokładnej kontroli klucza,
- złożoność zarządzania kluczami w dużych sieciach, co jest związane z kwadratową zależnością ilości kluczy, które trzeba generować, przekazywać, przechowywać i usuwać w sieci, od ilości użytkowników,
- złożoność wymiany kluczy, konieczność wstępnego przekazywania klucza.

Projektowanie algorytmów szyfrowania danych jest oparte na racjonalnym wyborze funkcji przekształcających oryginalne wiadomości do tekstu zaszyfrowanego. Ideę bezpośredniego zastosowania takiej funkcji do całej wiadomości realizuje się bardzo rzadko. Praktycznie wszystkie stosowane techniki kryptograficzne są związane z podziałem wiadomości na dużą liczbę fragmentów (czyli bloków) o ustalonym rozmiarze, z których każdy szyfruje się osobno. Takie podejście istotnie upraszcza zadanie szyfrowania i pozwala na szyfrowanie pakietów danych o nieograniczonej długości [4].

Szyfry blokowe są podstawą, na której realizują się prawie wszystkie systemy kryptograficzne, a ich cechami charakterystycznymi są szybkość oraz wydajność. W blokowych algorytmach kryptograficznych wszystkie wykonywane na danych działania oparte są na fakcie, że przetwarzany blok może być przedstawiony w postaci nieujemnej liczby całkowitej z zakresu odpowiadającego długości tego bloku.

Algorytm kryptograficzny jest uważany za idealnie odporny na deszyfrowanie, jeśli przeczytać zaszyfrowany blok danych można tylko przez sprawdzanie wszystkich możliwych kluczy, dopóki wiadomość nie okaże się zrozumiała. Zatem w ogólnym przypadku odporność szyfrów blokowych zależy od długości klucza i zwiększa się wykładniczo z jej wzrostem.

Wielomianowe modularne systemy liczbowe

Obecnie jakość realizacji procedur przetwarzania informacji zależy w dużym stopniu od wybranego modelu matematycznego organizacji tego procesu i zrealizowanej na jego podstawie technologii informacyjnej.

Istnieje szereg naukowych i praktycznych rodzajów działalności, gdzie występuje potrzeba przetwarzania informacji przedstawionych w formie wielomianów. Działania na wielomianach odgrywają istotną rolę we współczesnej algebrze komputerowej, cyfrowym przetwarzaniu sygnałów, teorii kodowania, kryptografii. W związku z tym duże zainteresowanie znajduje modularna technika równoległych struktur obliczeniowych zdefiniowanych w zakresach wielomianów.

Rozważmy zbiór $\boldsymbol{Z}[x]$ wszystkich wielomianów skończonego stopnia o współczynnikach z pierścienia liczb całkowitych $\boldsymbol{Z}$ i zmiennej x. W danym

przypadku technologia konstruowania modularnych systemów liczbowych (MSL) wymaga budowy pełnego systemu reszt (PSR) według wybieranych parami nawzajem prostych modułów wielomianowych $p_1(x), p_2(x), \ldots, p_n(x)$ [6, 8]. Zachodzi następujące twierdzenie.

Twierdzenie 1. W zbiorze $\boldsymbol{Z}[x]$ dla każdego wielomianu $f(x)$ i dowolnego modułu wielomianowego $p(x)$ o stopniu $\deg p(x) \geq 1$ istnieją jedyne elementy $q(x)$ i $r(x)$ takie, że

$$f(x) = q(x)\, p(x) + r(x)\ (\deg r(x) < \deg p(x)). \quad (1)$$

Ponieważ w aplikacjach komputerowych stosuje się skończone modele matematyczne, to dla budowy wielomianowych MSL (WMSL) zamiast zbioru $\boldsymbol{Z}[x]$ będziemy stosować zbiór $\boldsymbol{Z}_m[x]$ wszystkich wielomianów z pierścienia $\boldsymbol{Z}_m = \{0, 1, \ldots, m-1\}$. Niech $p(x)$ jest dowolnym elementem o stopniu s z $\boldsymbol{Z}_m[x]$. Wówczas zgodnie z twierdzeniem 1, które zachodzi i dla pierścienia $\boldsymbol{Z}_m[x]$, zbiorem wszystkich reszt $r(x)$ z dzielenia $f(x)$ przez $p(x)$ (patrz (1)), gdy $f(x)$ przebiega wszystkie elementy z $\boldsymbol{Z}_m[x]$, jest zbiór

$$\boldsymbol{Z}_m^s[x] = \left\{A(x) = \sum_{j=0}^{s-1} a_j x^j \,\middle|\, (a_0, a_1, \ldots, a_{s-1}) \in (\boldsymbol{Z}_m \times \boldsymbol{Z}_m \times \ldots \times \boldsymbol{Z}_m)\right\}, \quad (2)$$

gdzie m i s są stałe dodatnie liczby całkowite, $m \geq 2$. Moc zbioru (2) jest równa $N = |\boldsymbol{Z}_m^s[x]| = m^s$. Więc zbiór $\boldsymbol{Z}_m^s[x]$ jest PSR według modułu $p(x)$.
Dla oznaczenia PSR tego typu będziemy używać specjalnego zapisu $\langle\cdot\rangle_{p(x)}$, natomiast dla reszty $r(x)$ moduło $p(x)$ z wielomianu $f(x)$ będziemy używać zapisu $\langle f(x)\rangle_{p(x)}$.

W ogólnym przypadku WMSL z parami nawzajem prostych modułów wielomianowych $p_1(x), p_2(x), \ldots, p_n(x)$ indukuje się poprzez izomorficzne odwzorowanie $\varphi : \langle\cdot\rangle_{P(x)} \to \langle\cdot\rangle_{p_1(x)} \times \langle\cdot\rangle_{p_2(x)} \times \ldots \times \langle\cdot\rangle_{p_n(x)}$, gdzie $P(x) = \prod_{l=1}^{n} p_l(x)$, które każdemu wielomianowi $A(x) \in \langle\cdot\rangle_{P(x)}$ przyporządkowuje wielomianowy kod modularny (KM) $(a_1(x);\ a_2(x);\ \ldots;\ a_n(x))$, współrzędnymi którego są reszty $a_l(x) = \langle A(x)\rangle_{p_l(x)}$ $(l = 1, 2, \ldots, n)$ [8]. Zbiór $\langle\cdot\rangle_{P(x)}$ nazywa się zakresem WMSL.

Operacje pierścieniowe na dowolnych dwóch wielomianach:
$A(x) = (a_1(x);\ a_2(x);\ \ldots;\ a_n(x))$
i
$B(x) = \left(b_1(x);\ b_2(x);\ \ldots;\ b_n(x)\right)$ $(a_l(x) = \langle A(x)\rangle_{p_l(x)}, b_l(x) = \langle B(x)\rangle_{p_l(x)},$
$l = 1, 2, \ldots, n)$
według modułów wielomianowych $p_1(x), p_2(x), \ldots, p_n(x)$ są wykonywane niezależnie, czyli zgodnie z regułą

$$\langle A(x) \circ B(x)\rangle_{P(x)} = (\langle a_1(x) \circ b_1(x)\rangle_{p_1(x)},$$
$$\langle a_2(x) \circ b_2(x)\rangle_{p_2(x)}, \ldots, \langle a_n(x) \circ b_n(x)\rangle_{p_n(x)}\ (\circ \in \{+, -, \times\}) \quad (3)$$

Zatem, dodawanie i mnożenie dwóch dowolnych wielomianów według modułu $P(x)$ wymagają dla swojej realizacji odpowiednio n rzeczywistych dodawań i mnożeń, które ponadto mogą być wykonywane równolegle w jednym takcie modułowym. Wszystkie operacje tak modułowe (3), jak i niemodułowe w WMSL realizują się w pierścieniu $\boldsymbol{Z}_m$. Pierścień ten nazywa się skalarnym lub numerycznym zakresem WMSL.

Dekodujące odwzorowanie przyporządkowujące wielomianowemu KM $(a_1(x);\ a_2(x);\ \ldots; a_n(x))$ wielomian $A(x)$ z zakresu $\langle\cdot\rangle_{P(x)}$ realizuje się na podstawie Chińskiego twierdzenia o resztach [6], które dla WMSL z podstawami $p_l(x)$ $(l\ =\ 1, 2, \ldots, n)$ daje

$$A(x) = \langle\sum_{l=1}^{n} P_l(x)\langle P_l^{-1}(x)A(x)\rangle_{p_l(x)}\rangle_{P(x)} = \sum_{l=1}^{n} P_l(x)\langle P_l^{-1}(x)a_l(x)\rangle_{p_l(x)}, \qquad (4)$$

gdzie $P_l(x) = P(x)/p_l(x)$, $\langle P_l^{-1}(x)\rangle_{p_l(x)}$ jest resztą, dla której zachodzi równość $\langle P_l(x)\langle P_l^{-1}(x)\rangle_{p_l(x)}\rangle_{p_l(x)} = 1$.

Realizacja procesu szyfrowania informacji w WMSL

Rozważmy metodę szyfrowania w WMSL bardzo szybkiego strumienia danych. Sekwencja wejściowa, która stanowi zbiór symboli binarnych, jest podzielona na bloki o określonej długości (typowo 64, 128 lub więcej bitów). Każdy blok A dzieli się na s komponentów, tzn. można go zapisać w postaci $A = \{a_{s-1}, a_{s-2}, \ldots, a_1, a_0\}$, gdzie $a_j \in \boldsymbol{Z}_m$ $(j = 0, 1, \ldots, s - 1)$. Więc, początkowa długość bloku A powinna być wybrana zgodnie z warunkiem $L\ =\ l \times s$, gdzie $l\ =\ \lceil\log_2 m\rceil$ jest liczbą bitów dla przedstawienia komponentów a_j $\left(j = 0, 1, \ldots, s - 1\right)$ bloku, przez $\lceil x\rceil$ oznacza się najmniejszą liczbę całkowitą nie mniejszą niż x.

Zatem blok A w postaci wielomianu przedstawia się następująco:

$$A(x) = a_{s-1}x^{s-1} + a_{s-2}x^{s-2} + \cdots + a_2x^2 + a_1x^1 + a_0. \qquad (5)$$

W WMSL każdy blok $A(x)$ (5) jednoznacznie koduje się zbiorem reszt $a_l(x) = \langle A(x)\rangle_{p_l(x)}$ $(l\ =\ 1, 2, \ldots, n)$ według wybranych modułów wielomianowych $p_1(x),\ p_2(x), \ldots, p_n(x)$

$$A(x)\ =\ (a_1(x);\ a_2(x);\ \ldots;\ a_n(x)). \qquad (6)$$

Następnie do bloku $A(x)$ przedstawionego w wielomianowym KM stosuje się procedurę szyfrowania. W tym celu najpierw należy wygenerować sekwencję kluczową B o długości L bitów, która może być również przedstawiona w postaci wielomianu (patrz (5)), a następnie przekształcona do zbioru wielomianowych reszt $b_l(x) = \langle B(x)\rangle_{p_l(x)}$ $(l\ =\ 1, 2, \ldots, n)$ według stosowanych

modułów WMSL. W wyniku tego uzyskujemy wielomianowy KM sekwencji kluczowej B

$$B(x) = (b_1(x);\ b_2(x);\ \dots;\ b_n(x)). \tag{7}$$

Sam proces szyfrowania polega na nałożeniu sekwencji kluczowej na blok informacyjny w WMSL. Tę procedurę można rozpatrywać jak realizację pewnego przekształcenia $F(A(x), B(x))$, które wykonuje się równolegle według modułów wielomianowych systemu. Uzyskany kryptogram w WMSL ma postać

$$C(x) = \big(c_1(x);\ c_2(x);\ \dots;\ c_n(x)\big). \tag{8}$$

Przy użyciu różnych rodzajów przekształceń $F(A(x), B(x))$ mogą być otrzymane różne sposoby i algorytmy. Najprościej w WMSL realizują się operacje szyfrowania na podstawie formuły (3). Na przykład, kryptogram $C(x)$ (8) otrzymuje się poprzez mnożenie wielomianów (6) i (7).

$$C(x) = \langle A(x) \cdot B(x) \rangle_{P(x)}.$$

W tym przypadku współrzędne zbioru reszt $\big(c_1(x);\ c_2(x);\ \dots;\ c_n(x)\big)$ są najmniejszymi resztami z dzielenia iloczynów $a_l(x) \cdot b_l(x)$ przez odpowiednie moduły wielomianowe WMSL

$$c_l(x) = \langle a_l(x) \cdot b_l(x) \rangle_{p_l(x)}\ (l = 1, 2, \dots, n). \tag{9}$$

Żeby rozszyfrować kryptogram $C(x)$, potrzebny jest wielomian $B^{-1}(x) = (b_1^{-1}(x);\ b_2^{-1}(x);\ \dots; b_n^{-1}(x))$ odwrotny do wielomianu $B(x)$, który jest wielomianowym modularnym przedstawieniem wybranego klucza szyfru. Współrzędne $b_l^{-1}(x)$ wielomianowego KM oblicza się na podstawie równania

$$\langle b_l(x) \cdot b_l^{-1}(x) \rangle_{p_l(x)} = 1\ (l = 1, 2, \dots, n). \tag{10}$$

Wówczas wielomianowe przedstawienie wejściowego bloku $A(x)$ (6) można odzyskać zgodnie z (9) i (10) za pomocą następującej reguły

$$a_l(x) = \langle b_l^{-1}(x) \cdot c_l(x) \rangle_{p_l(x)}\ (l = 1, 2, \dots, n).$$

Więc, proces szyfrowania bloku danych o długości L bit w WMSL charakteryzuje się pełnym kluczem, który składa się z klucza szyfrowania $B(x)$ i zbioru wybranych modułów wielomianowych $p_1(x),\ p_2(x), \dots, p_n(x)$. Klucz odszyfrowania $B^{-1}(x)$ oblicza się zgodnie z (10). Obliczenie pozycyjnego kodu informacyjnego bloku A według jego wielomianowego KM $A(x)$ wykonuje się odpowiednio do formuły (4).

Przetwarzanie wielomianowych reszt w minimalnie nadmiernym KM

Z zależności (3) wynika, że poziom efektywności arytmetyki WMSL zależy tak od formy analitycznej podstaw $p_l(x)$ i ich stopni $\deg p_l(x)$ $(l = 1, 2, \ldots, n)$, jak i od systemu liczbowego, który wykorzystuje się dla realizacji obliczeń na resztach wielomianowych w pierścieniu $\boldsymbol{Z}_m$. Uwzględniając modułową strukturę tych obliczeń, dla kodowania i przetwarzania elementów z zakresu skalarów $\boldsymbol{Z}_m$ całkiem naturalnym wydaje się stosowanie rzeczywistej MSL z modułami $m_1, m_2, \ldots, m_k$ i zakresem przedstawienia liczb $M_k = \prod_{i=1}^{k} m_i$ [6, 7]. Przy takim podejściu parametr m przyjmuje wartość $m = M_k$, tj. pierścień $\boldsymbol{Z}_{M_k}$ stosuje się jako zakres liczbowy WMSL. Taki WMSL nazywa się wielomianowo-skalarnym MSL (WSMSL) [8].

Skuteczność arytmetyki komputerowej WSMSL znacznie się zwiększa, przy użyciu na dolnym poziomie minimalnie nadmiernego modularnego kodowania elementów z zakresu skalarów, co umożliwia optymalizację procedur niemodułowych. W tym przypadku WSMSL nazywa się minimalnie nadmiernym WSMSL.

Jak wiadomo, zasada minimalnie nadmiernego modularnego kodowania polega na tym, że jako zakres skalarów w WSMSL zamiast zbioru $\boldsymbol{Z}_{M_k}$ należy stosować zbiór $\boldsymbol{Z}_{2M}^{-} = \{-M, -M+1, \ldots, M-1\}$, gdzie $M = \prod_{i=0}^{k-1} m_i$, $m_k \geq 2m_0 + k - 2$, $m_0 \geq k - 2$ (m_0 jest pomocniczy moduł naturalny) [1, 9]. Więc, minimalnie nadmierny WSMSL definiuje się przez system parami nawzajem prostych wielomianów nierozkładalnych $p_1(x), p_2(x), \ldots, p_n(x)$ ze zbioru $\boldsymbol{Z}_{2M}^{-}$ oraz system parami nawzajem prostych liczb naturalnych $m_1, m_2, \ldots, m_k$.

Dla zastosowań praktycznych najbardziej wygodne są minimalnie nadmierne WSMSL z modułami wielomianowymi $p_1(x), p_2(x), \ldots, p_n(x)$, które są normowanymi wielomianami pierwszego stopnia: $p_l(x) = x - r_l$ $(r_l \in \boldsymbol{Z}_{2M}^{-}$; $l = 1, 2, \ldots, n)$, dla których $P(x) = \prod_{l=1}^{n} p_l(x) = x^n \pm 1$. W tym przypadku dowolny wielomian $A(x) \in \langle\cdot\rangle_{P(x)}$ koduje się zbiorem reszt

$$(\propto_{1,1}, \propto_{1,2}, \ldots, \propto_{1,k}\,;\ \propto_{2,1}, \propto_{2,2}, \ldots, \propto_{2,k}\,;\ldots;\ \propto_{n,1}, \propto_{n,2}, \ldots, \propto_{n,k}), \tag{11}$$

gdzie $\propto_{l,i} = |A_l|_{m_i}$; $A_l = \langle A(x)\rangle_{p_l(x)} = |A(r_l)|_{M_k}$; $|X|_m$ oznacza najmniejszą nieujemną resztę porównywalną z wartością X według modułu naturalnego m; $l = 1, 2, \ldots, n$; $i = 1, 2, \ldots, k$.

Minimalnie nadmierne WSMSL charakteryzują się strukturą równoległą tak na pierwszym, jak i na drugim kaskadzie operacji modułowych. Zgodnie z (3) operacje na dwóch dowolnych wielomianach $A(x)$ i $B(x)$ z zakresu $\langle\cdot\rangle_{P(x)}$ wykonuje się według reguły

$$\left(\propto_{1,1},\propto_{1,2},\ldots,\propto_{1,k}\,;\ \propto_{2,1},\propto_{2,2},\ldots,\propto_{2,k}\,;\ldots;\ \propto_{n,1},\propto_{n,2},\ldots,\propto_{n,k}\right)\circ$$
$$\left(\beta_{1,1},\beta_{1,2},\ldots,\beta_{1,k}\,;\ \beta_{2,1},\beta_{2,2},\ldots,\beta_{2,k}\,;\ldots;\ \beta_{n,1},\beta_{n,2},\ldots,\beta_{n,k}\right)=$$
$$(\left|\propto_{1,1}\circ\beta_{1,1}\right|_{m_1},\left|\propto_{1,2}\circ\beta_{1,2}\right|_{m_2},\ldots,\left|\propto_{1,k}\circ\beta_{1,k}\right|_{m_k};$$
$$\left|\propto_{2,1}\circ\beta_{2,1}\right|_{m_1},\left|\propto_{2,2}\circ\beta_{2,2}\right|_{m_2},\ldots,\left|\propto_{2,k}\circ\beta_{2,k}\right|_{m_k};\ldots;$$
$$\left|\propto_{n,1}\circ\beta_{n,1}\right|_{m_1},\left|\propto_{n,2}\circ\beta_{n,2}\right|_{m_2},\ldots,\left|\propto_{n,k}\circ\beta_{n,k}\right|_{m_k}),\qquad(12)$$

gdzie reszty $\propto_{l,i}=|A(r_l)|_{m_i}$ i $\beta_{l,i}=|B(r_l)|_{m_i}$ są cyframi wielomianowo-skalarnych KM operandów $A(x)$ i $B(x)$ odpowiednio (patrz (11)), $\circ\in\{+,-,\times\}$ [8].

Jedna z głównych zalet WSMSL polega na unikalnej możliwości obliczenia zgodnie z (12) sumy, różnicy i przede wszystkim iloczynu dwóch wielomianów w ciągu jednego taktu modułowego. W przypadku stosowania tradycyjnej arytmetyki pozycyjnej w pierścieniu $\langle\cdot\rangle_{P(x)}$ przy mnożeniu dwóch wielomianów złożoność obliczeniowa składa się z $n(n-1)$ rzeczywistych dodawań i n^2 rzeczywistych mnożeń.

Jest oczywiste, że istotny wpływ na realny efekt od wprowadzenia do praktyki wielomianowej arytmetyki modularnej może mieć wydajność stosowanych metod przekształcenia wielomianów z pozycyjnego systemu liczbowego w WSMSL i na odwrót oraz metoda wykonywania na wielomianach innych operacji niemodułowych [1].

Wskazany problem skutecznie się rozwiązuje przy użyciu minimalnie nadmiernego modularnego kodowania skalarów z zakresu $\boldsymbol{Z}_{2M}^{-}$. Rozważmy najpierw operację obliczenia cyfr wielomianowo-skalarnych KM. W szczególności, dla cyfr $\propto_{l,i}$ kodu (11) dowolnego wielomianu $A(x)=\sum_{\nu=0}^{n-1}a_\nu x^\nu$ z zakresu $\langle\cdot\rangle_{P(x)}$ ($a_\nu\in\boldsymbol{Z}_{2M}^{-}$) zachodzi wzór

$$\propto_{l,i}=\left|\sum_{\nu=0}^{n-1}R_{\nu,l,i}\sum_{s=0}^{\mu-1}\left|F_s(a_\nu^{(s)})\right|_{m_i}\right|_{m_i}\quad(l=1,2,\ldots,n;\ i=1,2,\ldots,k),$$

gdzie $R_{\nu,l,i}=|r_l^\nu|_{m_i}$; $F_s(a_\nu^{(s)})$ są addytywne współrzędne λ - bitowych pozycyjnych form współczynników a_ν:

$$a_\nu=\sum_{t=0}^{\lambda-1}a_{\nu,t}2^t-a_{\nu,\lambda-1}2^\lambda=\sum_{t=0}^{\lambda-2}a_{\nu,t}2^t-a_{\nu,\lambda-1}2^{\lambda-1}=\sum_{s=0}^{\mu-1}F_s(a_\nu^{(s)}),$$

które definiowane są według formuł

$$a_\nu^{(s)} = \sum_{t=0}^{\lambda_s - 1} a_{\nu, q_s + t} 2^t \ (s = 0, 1, \ldots, \mu - 1),$$

$$F_s\left(a_\nu^{(s)}\right) = \begin{cases} a_\nu^{(s)} 2^{q_s} \text{ gdy } s = 0, 1, \ldots, \mu - 2, \\ a_\nu^{(\mu-1)} 2^{q_{\mu-1}} - \left\lfloor a_\nu^{(\mu-1)} / 2^{q_{\mu-1}-1} \right\rfloor 2^\lambda \text{ gdy } s = \mu - 1; \end{cases}$$

$q_0 = 0, q_1, \ldots, q_{\mu-1}$ jest rosnąca sekwencja wartości całkowitych, która określa podział kodu binarnego $(a_{\nu,\lambda-1}, a_{\nu,\lambda-2}, \ldots, a_{\nu,0})_2$ na $\mu \geq 1$ grup, *s*-ta z których zawiera $\lambda_s = q_{s+1} - q_s$ bitów, $q_{\mu-1} \leq \lambda - 1$, $q_\mu = \lambda$, przez $\lfloor y \rfloor$ oznacza się część całkowita liczby rzeczywistej y.

Żeby obliczyć cyfry pozycyjnego przedstawienia wielomianu $A(x)$ według jego wielomianowo-skalarnego KM (11), należy najpierw dla każdego $\nu = 0, 1, \ldots, n-1$ uzyskać minimalnie nadmierny MK $\left(\alpha_1^{(\nu)}, \alpha_2^{(\nu)}, \ldots, \alpha_k^{(\nu)}\right)$ współczynnika a_ν [8]:

$$\alpha_i^{(\nu)} = |a_\nu|_{m_i} = \left| \sum_{l=1}^{n} R_{l,i}^{(\nu)} \propto_{l,i} \right|_{m_i} \ (i = 1, 2, \ldots, k),$$

gdzie $R_{l,i}^{(\nu)} = |n^{-1} r_l^{-\nu}|_{m_i}$. Następnie kod pozycyjny współczynnika a_ν może być obliczony na podstawie jego KM na podstawie wzoru

$$a_\nu = \sum_{i=1}^{k-1} M_{i,k-1} \left| M_{i,k-1}^{-1} \alpha_i^{(\nu)} \right|_{m_i} + I(a_\nu) M_{k-1},$$

gdzie $M_{i,k-1} = M_{k-1}/m_i$, $M_{k-1} = \prod_{j=1}^{k-1} m_i$, $I(a_\nu)$ to wartość całkowita, zwana przedziałowym indeksem liczby a_ν, którą oblicza się według wzorów [1, 9]

$$I(a_\nu) = \begin{cases} \hat{I}_k(a_\nu), \text{jeśli } \hat{I}_k(a_\nu) < m_0, \\ \hat{I}_k(a_\nu) - m_k, \text{jeśli } \hat{I}_k(a_\nu) \geq m_k - m_0 - k + 2; \end{cases}$$

$$\hat{I}_k(a_\nu) = \left| \sum_{i=1}^{k} R_{i,k}(\alpha_i^{(\nu)}) \right|_{m_k},$$

$$R_{i,k}\left(\alpha_i^{(\nu)}\right) = \left| \frac{\left| M_{i,k-1}^{-1} \alpha_i^{(\nu)} \right|_{m_i}}{M_{k-1}} \right|_{m_k} \ (i \neq k), \ R_{k,k}\left(\alpha_i^{(\nu)}\right) = \left| \frac{\alpha_k^{(\nu)}}{M_{k-1}} \right|_{m_k}.$$

Więc, przy użyciu minimalnie nadmiernego kodowania na dolnym poziomie efektywność arytmetyki komputerowej WSMSL znacznie się zwiększa kosztem optymalizacji procedur niemodułowych. Zatem arytmetyce minimalnie nadmiernych WSMSL potencjalnie należą się priorytetowe pozycje w dziedzinie zastosowań komputerowych.

Proponowane opracowania pozwalają przy dość prostej realizacji stwarzać efektywne systemy i środki ochrony kryptograficznej na podstawie blokowego symetrycznego algorytmu szyfrowania danych z użyciem minimalnie nadmiernych WSMSL. W takich systemach na górnym poziomie stosuje się normalizowane wielomiany pierwszego stopnia, a na dolnym poziomie stosuje się minimalnie nadmierne modularne kodowanie elementów z zakresu skalarów.

Ponadto możemy zauważyć, że w ramach opracowanej technologii tworzenia MSL można zdefiniować minimalnie nadmierne WSMSL z zakresami skalarów zespolonych [5, 7]. Uzyskane w tym przypadku zwiększenie wydajności w porównaniu do tradycyjnych realizacji jest jeszcze bardziej imponujące niż w przypadku rzeczywistych WSMSL.

Literatura

[1] Czerniawski A.F. (red.), Bardzo szybkie metody i systemy cyfrowego przetwarzania informacji, Białoruski uniwersytet państwowy, Mińsk, 1996, (w języku rosyjskim).
[2] Ferguson N., Schneier B., Kryptografia w praktyce, Helion, Gliwice, 2004.
[3] Karbowski M., Podstawy kryptografii. Wydanie II, Helion, Gliwice, 2008.
[4] Pieprzyk J., Hardjono T., J. Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion, Gliwice, 2005.
[5] Selyaninov M., Arithmetic of quadratic minimal redundant modular number systems, Jan Dlugosz University of Czestochowa. Scientific Issues, Mathematics XVI, Czestochowa, 2011, p. 129-134.
[6] Selyaninov M., Construction of modular number systems with arbitrary finite ranges, Jan Dlugosz University of Czestochowa. Scientific Issues, Mathematics XIV, Czestochowa, 2009, p. 105-115.
[7] Selyaninov M., Modular number systems in a complex plane, Jan Dlugosz University of Czestochowa. Scientific Issues, Mathematics XV, Czestochowa, 2010, p. 131-138.
[8] Selyaninov M., Modular technique of high-speed parallel computing on the sets of polynomials, Jan Dlugosz University of Czestochowa. Scientific Issues, Mathematics XVII, Czestochowa, 2012, p. 69-76.
[9] Selianinau M., Modular technique of parallel information processing, Jan Dlugosz University of Czestochowa. Scientific Issues, Mathematics XII, Czestochowa, 2008, p. 43-52.